ALGEBRA I

Kevad 2015

Lektor: Valdis Laan

Sisukord

Eessõna

Algebra kui matemaatikaharu võib jagada kaheks suureks osaks: lineaaralgebraks ja abstraktseks algebraks. Käesolev kursus koosneb põhiliselt lineaaralgebrast: vaatleme maatrikseid, determinante, lineaarvõrrandisüsteeme, vektorruume ja lineaarkujutusi. Abstraktne algebra uurib algebralisi struktuure. Struktuuridest tutvume vaid väga põgusalt kõige tähtsamatega: rühma, ringi ja korpusega.

Kursuse jooksul eeldame, et üliõpilane on tuttav selliste hulgateooria põhimõistetega nagu alamhulk, hulkade otsekorrutis, ühisosa, ühend, kujutus, binaarne seos, ekvivalentsiseos, ekvivalentsiklass. Samuti eeldame, et kuulajale on tuttavad naturaalarvude, täisarvude, ratsionaalarvude ja reaalarvude omadused.

Seda teksti lugedes panete tähele, et mõned kohad tekstis on väiksemas kirjas kui ülejäänud tekst. Nende kohtade lugemine ei ole muust materjalist arusaamiseks vajalik.

Kursuse jooksul kasutame mitmeid matemaatilisi ja matemaatilise loogika sümboleid, mille tähendused on järgmised:

$\forall a \in A$ — iga elemendi a korral hulgast A ehk hulga A iga elemendi a korral;

$\exists a \in A$ — leidub element a hulgas A ehk leidub hulga A element a;

$A \Rightarrow B$ — A-st järeldub B;

$A \Leftrightarrow B$ — A kehtib parajasti siis, kui kehtib B, ehk A kehtib siis ja ainult siis, kui kehtib B;

$\mathbb{N}$ — naturaalarvude hulk;

$\mathbb{Z}$ — täisarvude hulk;

$\mathbb{Q}$ — ratsionaalarvude hulk;

$\mathbb{R}$ — reaalarvude hulk.

1 Maatriksid

1.1 Sissejuhatus

Vaatleme ühte lihtsat lineaarvõrrandisüsteemi

$$\begin{cases} 2x & + & 3y & = & 7 \\ 4x & - & y & = & -7 \end{cases}.$$

Lahendame selle järgneval viisil. Kõigepäält lahutame teise võrrandi vastavatest pooltest esimese võrrandi vastavad pooled, mis on korrutatud kahega. Saame süsteemi

$$\begin{cases} 2x & + & 3y & = & 7 \\ & - & 7y & = & -21 \end{cases}.$$

Korrutades teise võrrandi mõlemad pooled arvuga $-\frac{1}{7}$ saame

$$\begin{cases} 2x & + & 3y & = & 7 \\ & & y & = & 3 \end{cases}.$$

Nüüd lahutame esimese võrrandi vastavatest pooltest teise võrrandi vastavad pooled, mis on korrutatud 3-ga. See annab meile süsteemi

$$\begin{cases} 2x & & = & -2 \\ & y & = & 3 \end{cases}.$$

Lõpuks korrutame veel esimese võrrandi mõlemad pooled arvuga $\frac{1}{2}$ ja saamegi lahendi

$$\begin{cases} x & & = & -1 \\ & y & = & 3 \end{cases}.$$

Teeme siinkohal mõned tähelepanekud. Esiteks, süsteemi lahendamiseks oli meil vaja ainult kahte tüüpi teisendusi:

- süsteemi mingile võrrandile mingi arvuga korrutatud teise võrrandi liitmine;
- mingi võrrandi korrutamine mingi nullist erineva arvuga.

Kogu lahenduskäik põhineb asjaolul, et teisenduse tulemusena saadud süsteemil on täpselt samad lahendid, mis esialgsel. Kuna viimast süsteemi rahuldab ilmselt ainult arvupaar $(-1, 3)$, siis on see ka esialgse süsteemi ainus lahend.

Teiseks paneme tähele, et paigutades tundmatute x ja y kordajad ning vabaliikmed kahe rea ja kolme veeruga tabelisse võime kogu lahenduskäigu esitadagi ainult selliste tabelite abil:

$$\begin{pmatrix} 2 & 3 & 7 \\ 4 & -1 & -7 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 7 \\ 0 & -7 & -21 \end{pmatrix} \to \begin{pmatrix} 2 & 3 & 7 \\ 0 & 1 & 3 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix}.$$

Siin on kõigis tabelites esimeses veerus x kordajad, teises veerus y kordajad ja kolmandas veerus vabaliikmed. Tabeli esimene rida vastab süsteemi esimesele võrrandile ja teine rida teisele võrrandile. Tabel on ümbritsetud ümarsulgudega. On selge, et sellise tähistuse juures saab alati võrrandisüsteemi põhjal välja kirjutada vastava tabeli ja vastupidi, tabeli järgi on alati võimalik taastada süsteem. Tabeli eelis on see, et pole vaja näha vaeva tundmatute ja võrdusmärkide kirjutamisega.

Selles kursuses ongi meie üheks eesmärgiks õppida lahendama lineaarvõrrandisüsteeme, kus tundmatuid ja võrrandeid ei ole mitte kaks, vaid suvaline lõplik arv, kusjuures tundmatute ja võrrandite arv võib olla erinev. Lahendamise juures kasutatakse tänapäeva matemaatikas justnimelt ülalkirjeldatud tabeleid, neid nimetatakse maatriksiteks.

Lineaarvõrrandisüsteemide lahendamise vajadus tekib matemaatikas väga paljudes kohtades. Näiteks saab nende abil leida vektori koordinaate baasi suhtes, lineaarteisenduse omavektoreid, avaldada sümmeetrilisi polünoome sümmeetriliste põhipolünoomide kaudu jne. Samuti on lineaarvõrrandisüsteeme tarvis suure hulga praktiliste ülesannete lahendamisel.

Vaatame veel mõningaid näiteid.

Näide 1.1 Üheks põhiviisiks piltide käsitlemiseks arvutis on rastergraafika (inglise keeles *raster graphics*). Selle lähenemise põhiidee on selline, et pilt jagatakse pisikesteks ruudukesteks (piksliteks), millest igaüks asub kindla rea ja veeru lõikekohas ja millel on kindel värv, mis on kodeeritud arvuna. Seega rasterpilti võib vaadelda kui ristkülikukujulist arvutabelit.

Näide 1.2 Olgu $G = (V, E)$ lõplik mittesuunatud silmusteta ja kordsete servadeta graaf tippude hulgaga $V = \{v_1, \ldots, v_n\}$. Graafiga G saab siduda $(n \times n)$-tabeli nii, et i-nda rea ja j-nda veeru lõikekohas on 1, kui $(v_i, v_j) \in E$ (s.t. kui tippude v_i ja v_j vahel on serv graafis G), vastasel juhul on sellel kohal 0. Selliseid tabeleid kasutatakse graafiteoorias ja neid nimetatakse **graafide naabrusmaatriksiteks**.

1.2 Maatriksi mõiste

Definitsioon 1.3 Olgu m ja n naturaalarvud. **$(m \times n)$-maatriks** on m reast ja n veerust koosnev tabel, mille iga rea ja iga veeru lõikekohal on mingi reaalarv ja mis on ümbritsetud ümarsulgudega. Neid reaalarve nimetatakse **maatriksi elementideks**. Kõigi $(m \times n)$-maatriksite hulka tähistatakse $\mathrm{Mat}_{m,n}$ või $\mathrm{Mat}_{m,n}(\mathbb{R})$.

Märkus 1.4 Siin me vaatleme lihtsuse mõttes esialgu ainult reaalarvuliste elementidega maatrikseid. Matemaatikas kasutatakse palju ka maatrikseid, mille elementidele sellist piirangut ei seata, elemendid on kas mingist korpusest või isegi ringist (vt. definitsiooni 4.14 ja 4.12).

Näide 1.5 Näiteks

$$\begin{pmatrix} 2 & 3 & 7 & 0 \\ 4 & -1 & -7 & 5 \end{pmatrix}, \quad \begin{pmatrix} 6 & -4 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

on vastavalt (2×4)-, (2×2)- ja (3×1)-maatriksid. Neist esimese maatriksi 1. rea ja 3. veeru element (ehk element kohal $(1, 3)$) on 7.

Maatrikseid tähistatakse harilikult suurte ladina tähtede $A, B, C, \ldots$ abil. Rääkides maatriksist üldiselt tähistatakse tema elemente harilikult väikese ladina tähe abil, millel on kaks indeksit. Neist esimene näitab, millises reas vaadeldav element asub ja teine näitab, millises veerus see element on. Näiteks $(m \times n)$-maatriks A, mille elemendid on a_{ij}, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, esitatakse harilikult kujul

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

või

$$A = (a_{ij})_{i=1,\ldots,m, j=1,\ldots,n}.$$

Kui kontekstist on selge, millised on A mõõtmed (s.o. ridade arv ja veergude arv), siis kirjutatakse lühidalt ka

$$A = (a_{ij}).$$

Märkus 1.6 Maatriksit $A \in \mathrm{Mat}_{m,n}$ on võimalik vaadelda kui kujutust $A : \{1, \ldots, m\} \times \{1, \ldots, n\} \longrightarrow \mathbb{R}$. Sellise lähenemise korral on a_{ij} järjestatud paari (i, j) kujutis, s.t. $a_{ij} = A(i, j)$. Siiski praktika on näidanud, et maatriksite käsitlemine tabelitena on palju mugavam ja otstarbekam.

Definitsioon 1.7 Kaks maatriksit on **võrdsed**, kui nende ridade arvud on võrdsed, veergude arvud on võrdsed ja vastavatel kohtadel olevad elemendid on võrdsed.

Seega maatriksid $A = (a_{ij})$ ja $B = (b_{ij})$ hulgast $\mathrm{Mat}_{m,n}$ on võrdsed parajasti siis, kui $a_{ij} = b_{ij}$ iga $i \in \{1, \ldots, m\}$ ja $j \in \{1, \ldots, n\}$ korral.

Definitsioon 1.8 Ruutmaatriks on maatriks, mille ridade arv on võrdne veergude arvuga. Kui maatriksis on n rida ja n veergu, siis öeldakse, et see on **n-ndat järku ruutmaatriks.**

Kõigi n-ndat järku ruutmaatriksite hulka tähistatakse Mat_n. Näiteks $\begin{pmatrix} 5 & 1 \\ -1 & 3 \end{pmatrix} \in \mathrm{Mat}_2$.

Definitsioon 1.9 Kui $A = (a_{ij}) \in \mathrm{Mat}_n$, siis öeldakse, et elemendid $a_{11}, a_{22}, \ldots, a_{nn}$ moodustavad maatriksi A **peadiagonaali**.

Eelmise näitemaatriksi peadigonaal koosneb seega arvudest 5 ja 3.

Iga maatriksiga saab loomulikul viisil siduda veel kaks maatriksit: transponeeritud maatriksi ja vastandmaatriksi.

Transponeerimine tähendab maatriksi ridade ja veergude ümbervahetamist.

Definitsioon 1.10 Maatriksi A **transponeeritud maatriks** on maatriks, mille esimeseks reaks on maatriksi A esimene veerg, teiseks reaks maatriksi A teine veerg jne. Tähistus: A^T või A^t.

Definitsioonist on selge, et kui $A \in \mathrm{Mat}_{m,n}$, siis $A^T \in \mathrm{Mat}_{n,m}$. Samuti on ilmne, et

$$(A^T)^T = A.$$

Näide 1.11 Näiteks

$$\begin{pmatrix} 2 & 3 & 7 & 0 \\ 4 & -1 & -7 & 5 \end{pmatrix}^T = \begin{pmatrix} 2 & 4 \\ 3 & -1 \\ 7 & -7 \\ 0 & 5 \end{pmatrix}.$$

Definitsioon 1.12 Maatriksi $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ **vastandmaatriksiks** $-A$ nimetatakse maatriksit, mille elementideks on maatriksi A vastavate elementide vastandarvud, s.t. maatriksit

$$-A = \begin{pmatrix} -a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & -a_{22} & \ldots & -a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ -a_{m1} & -a_{m2} & \ldots & -a_{mn} \end{pmatrix}.$$

Definitsioonist on selge, et kui $A \in \mathrm{Mat}_{m,n}$, siis $-A \in \mathrm{Mat}_{m,n}$ ja $-(-A) = A$.

Näide 1.13 Näiteks kui

$$A = \begin{pmatrix} 2 & 3 & 7 & 0 \\ 4 & -1 & -7 & 5 \end{pmatrix},$$

siis

$$-A = \begin{pmatrix} -2 & -3 & -7 & 0 \\ -4 & 1 & 7 & -5 \end{pmatrix}.$$

Nende mõistete abil defineeritakse sümmeetrilised ja kaldsümmeetrilised maatriksid.

Definitsioon 1.14 Ruutmaatriks A on **sümmeetriline**, kui $A^T = A$. Ruutmaatriks A on **kaldsümmeetriline**, kui $A^T = -A$.

Näide 1.15 Maatriks

$$A = \begin{pmatrix} 2 & 3 & 7 \\ 3 & -1 & -7 \\ 7 & -7 & 4 \end{pmatrix}$$

on sümmeetriline ja maatriks

$$B = \begin{pmatrix} 0 & -3 & 1 \\ 3 & 0 & -2 \\ -1 & 2 & 0 \end{pmatrix}$$

on kaldsümmeetriline.

Niisiis ruutmaatriks on sümmeetriline, kui tema peadiagonaali (kui mõttelise joone) suhtes sümmeetriliselt asuvad elemendid on võrdsed.

1.3 Reaalarvudest ja summeerimisest

Kuna paljud maatriksite omadused järelduvad reaalarvude omadustest, siis kordame üle, mida me teame reaalarvude kohta. Eeldame, et reaalarvu mõiste on lugejale tuttav. Samuti teame, et kahel reaalarvul on alati olemas summa ja korrutis, igal reaalarvul on olemas vastandarv ja igal nullist erineval reaalarvul leidub pöördarv.

Lause 1.16 *Reaalarvude liitmisel ja korrutamisel on järgmised omadused:*

RA1. $(a+b)+c = a+(b+c)$ *iga* $a, b, c \in \mathbb{R}$ *korral* *(s.t. liitmine on assotsiatiivne);*

RA2. *reaalarv* 0 *on selline, et* $a + 0 = a = 0 + a$ *iga* $a \in \mathbb{R}$ *korral;*

RA3. *iga* $a \in \mathbb{R}$ *korral on arv* $-a \in \mathbb{R}$ *selline, et* $a + (-a) = 0 = (-a) + a$*;*

RA4. $a + b = b + a$ *iga* $a, b \in \mathbb{R}$ *korral* *(liitmine on kommutatiivne);*

RA5. $(ab)c = a(bc)$ *iga* $a, b, c \in \mathbb{R}$ *korral* *(korrutamine on assotsiatiivne);*

RA6. *reaalarv* 1 *on selline, et* $a1 = a = 1a$ *iga* $a \in \mathbb{R}$ *korral;*

RA7. $a(b+c) = ab + ac$ *iga* $a, b, c \in \mathbb{R}$ *korral* *(distributiivsuse seadus);*

RA8. *iga* $a \in \mathbb{R} \setminus \{0\}$ *korral on arv* $\frac{1}{a} \in \mathbb{R}$ *selline, et* $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$*;*

RA9. $ab = ba$ *iga* $a, b \in \mathbb{R}$ *korral* *(korrutamine on kommutatiivne).*

Siin loetletud omadused ei ole kindlasti ainsad, mis reaalarvudel on. Näiteks omadustest RA7 ja RA9 järeldub (kuidas!), et

$$(a+b)c = ac + bc$$

iga $a, b, c \in \mathbb{R}$ korral. Vastavalt sellele, kuidas defineeritakse vastandarvud ja korrutamine, kehtib iga $a \in \mathbb{R}$ korral võrdus

$$-a = (-1)a. \tag{1}$$

Samuti teame, et reaalarvude lahutamine on defineeritud vastandarvu liitmise abil, s.t.

$$a - b = a + (-b). \tag{2}$$

Seega saab näiteks tõestada, et

$$a(-b) = -ab \tag{3}$$

ja $a(b-c) = ab - ac$. Tõepoolest,

$$a(-b) \underset{(1)}{=} a((-1)b) \underset{RA5}{=} (a(-1))b \underset{RA9}{=} ((-1)a)b \underset{RA5}{=} (-1)(ab) \underset{(1)}{=} -ab$$

ja

$$a(b-c) \underset{(2)}{=} a(b+(-c)) \underset{RA7}{=} ab + a(-c) \underset{(3)}{=} ab + (-ac) \underset{(2)}{=} ab - ac.$$

Toome sisse veel ühe tähistuse, mida matemaatikas kasutatakse palju ja mis aitab meil mitmetes kohtades materjali lihtsamalt esitada. Nimelt summat $s_1 + s_2 + s_3 + \ldots + s_n$ $(n \in \mathbb{N})$ tähistatakse lühidalt

$$\sum_{i=1}^{n} s_i. \tag{4}$$

Siin $\sum$ (kreeka suurtäht sigma) on summeerimismärk ja i on summeerimisindeks. Arvud 1 ja n näitavad ära, millistes piirides summeerimisindeks muutub ja summeerimisindeks omandab kõik naturaalarvulised väärtused 1-st n-ni. Igale i väärtusele vastab üks liidetav vaadeldavas summas. Liidetavate s_i tähendus sõltub kontekstist. Harilikult me summeerime reaalarve, aga summeerida võib ka teistsuguseid matemaatilisi objekte. Avaldist (4) võiks lugeda järgmiselt: "summa, kus i muutub ühest n-ni, s_i-dest" või "s_i-de summa, kus i muutub ühest n-ni".

Näiteks kui $s_1 = 2$, $s_2 = 1$, $s_3 = -4$ ja $s_4 = 5$, siis

$$\sum_{i=1}^{4} s_i = 2 + 1 - 4 + 5 = 4.$$

Liidetav s_i võib olla ka mingi avaldis, mis sõltub arvust i. Näiteks

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 + n^2.$$

Võib vaadelda ka summasid, kus liidetavad sõltuvad kahest indeksist. Selliseid liidetavaid võib summeerida kas ühe, teise või mõlema indeksi järgi. Näiteks võib vaadelda summat

$$\sum_{i=1}^{m} \sum_{j=1}^{n} s_{ij},$$

kus liidetavaid s_{ij} summeritakse enne j ja siis i järgi. Sellise summa erijuhuks on näiteks

$$\sum_{i=1}^{2}\sum_{j=1}^{3} j^i = \sum_{i=1}^{2}(1^i + 2^i + 3^i) = (1^1 + 2^1 + 3^1) + (1^2 + 2^2 + 3^2) = 6 + 14 = 20.$$

Summeerimismärki võib kasutada ka sellistel juhtudel, kui on vaja summeerida mingisse hulka kuuluvaid reaalarve. Kui näiteks A on kõigi 10-st väiksemate algarvude hulk, siis

$$\sum_{a\in A}(a-5) = (2-5) + (3-5) + (5-5) + (7-5) = -3 - 2 + 0 + 2 = -3.$$

Lause 1.17 *Reaalarvude summeerimisel on järgmised omadused:*

SO1.

$$\boxed{\sum_{i=1}^{n} ts_i = t\sum_{i=1}^{n} s_i}$$

(s.t. konstandi, mis ei sõltu summeerimisindeksist, võib tuua summa märgi ette);

SO2.

$$\boxed{\sum_{i=1}^{n}(s_i + t_i) = \sum_{i=1}^{n} s_i + \sum_{i=1}^{n} t_i;}$$

SO3.

$$\boxed{\sum_{i=1}^{m}\sum_{j=1}^{n} s_{ij} = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} s_{ij}\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} s_{ij}\right)}$$

(s.t. summeerimise järjekorda võib vahetada).

Tõestus. SO1 järeldub reaalarvude distributiivsuse omadusest RA7.

SO2. Tõepoolest,

$$\begin{aligned}\sum_{i=1}^{n}(s_i + t_i) &= (s_1 + t_1) + (s_2 + t_2) + \ldots + (s_n + t_n)\\ &\underset{RA1,RA4}{=} (s_1 + s_2 + \ldots + s_n) + (t_1 + t_2 + \ldots + t_n)\\ &= \sum_{i=1}^{n} s_i + \sum_{i=1}^{n} t_i.\end{aligned}$$

SO3. Paneme tähele, et

$$\begin{aligned}\sum_{i=1}^{m}\left(\sum_{j=1}^{n} s_{ij}\right) &= \sum_{i=1}^{m}(s_{i1} + \ldots + s_{in})\\ &= (s_{11} + \ldots + s_{1n}) + (s_{21} + \ldots + s_{2n}) + \ldots + (s_{m1} + \ldots + s_{mn})\\ &\underset{RA1,RA4}{=} (s_{11} + s_{21} + \ldots + s_{m1}) + \ldots + (s_{1n} + s_{2n} + \ldots + s_{mn})\\ &= \sum_{j=1}^{n}(s_{1j} + \ldots + s_{mj})\\ &= \sum_{j=1}^{n}\left(\sum_{i=1}^{m} s_{ij}\right).\end{aligned}$$

Kuna liidetavaid s_{ij} võime vaadelda kui $(m \times n)$-maatriksi elemente, siis vaadeldavat omadust võib tõlgendada nii, et maatriksi kõigi elementide summa ei sõltu sellest, kas me liidame neid järjest ridade kaupa või veergude kaupa. □

1.4 Maatriksite liitmine ja maatriksi korrutamine arvuga

Nagu eespool nägime, saab maatrikseid kasutada selleks, et struktureeritult esitada informatsiooni, näiteks lineaarvõrrandisüsteemi kordajaid ja vabaliikmeid. Siiski maatriksite teooria kogu kasulikkus ja võimsus avaldub tänu sellele, et maatriksitega on võimalik teha tehteid: sobivate mõõtmetega maatrikseid on võimalik omavahel liita, korrutada ja iga maatriksit võib korrutada arvuga.

Enne tehete juurde asumist peatume veelkord sellel, kuidas on võimalik maatrikseid esitada. Me võime näiteks vaadelda maatriksit $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$, mille element a_{ij}, kus $i \in \{1, \ldots, m\}$ ja $j \in \{1, \ldots, n\}$, on antud mingi valemiga, mis võib sõltuda indeksitest i ja j. Näiteks maatriks $A = (a_{ij}) \in \mathrm{Mat}_{3,4}$, kus

$$a_{ij} = \min(4, i + j),$$

näeb välja nii:

$$A = \begin{pmatrix} 2 & 3 & 4 & 4 \\ 3 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix}.$$

Tihti kirjutatakse sama asja veel lühemalt: $A = (\min(4, i + j)) \in \mathrm{Mat}_{3,4}$. See kirjapilt väljendab järgmist asjaolu: A on (3×4)-maatriks, mille i-ndas reas ja j-ndas veerus on arv $\min(4, i + j)$.

Kui $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$, siis $B = (a_{ij} + 3) \in \mathrm{Mat}_{m,n}$ on $(m \times n)$-maatriks, mille i-ndas reas ja j-ndas veerus on arv $a_{ij} + 3$. Samasugust kokkulepet kasutades võime öelda, et

$$-A = (-a_{ij}) \in \mathrm{Mat}_{m,n}$$

ja

$$A^T = (a_{ji}) \in \mathrm{Mat}_{n,m}.$$

Väga tihti läheb lineaaralgebras vaja järgmisi mingis mõttes hästi lihtsaid maatrikseid.

Definitsioon 1.18 **Nullmaatriks** on maatriks, mille kõik elemendid on nullid.

Definitsioon 1.19 **Ühikmaatriks** on ruutmaatriks, mille peadiagonaalil on ühed ja kõik muud elemendid on nullid.

$(m \times n)$-nullmaatriksit tähistame sümboliga $\Theta_{m,n}$ või lihtsalt Θ (kreeka suurtäht teeta). Tihti kasutatakse nullmaatriksi tähisena ka lihtsalt sümbolit 0.

n-ndat järku ühikmaatriksit tähistame sümboliga E_n või lihtsalt E. Kasutatakse ka tähist I_n.

Näide 1.20 Näiteks

$$\Theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{ja} \quad E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

on vastavalt (3×2)-nullmaatriks ja kolmandat järku ühikmaatriks.

Üldjuhul võib kirjutada ka

$$\Theta_{m,n} = (\theta_{ij}), \text{ kus } \theta_{ij} = 0 \text{ iga } i \in \{1,\dots,m\}, j \in \{1,\dots,n\} \text{ korral}$$

ja

$$E_n = (\delta_{ij}), \text{ kus } \delta_{ij} = \begin{cases} 1, & \text{kui } i = j, \\ 0, & \text{kui } i \neq j, \end{cases} \text{ iga } i,j \in \{1,\dots,n\} \text{ korral.}$$

Sümbolit δ_{ij} tuntakse matemaatikas kui **Kroneckeri**[1] **deltat**.

Defineerime nüüd maatriksite summa.

Definitsioon 1.21 Maatriksite $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ ja $B = (b_{ij}) \in \mathrm{Mat}_{m,n}$ **summa** on maatriks $A + B = (c_{ij}) \in \mathrm{Mat}_{m,n}$, kus $c_{ij} = a_{ij} + b_{ij}$ iga $i \in \{1,\dots,m\}$ ja $j \in \{1,\dots,n\}$ korral.

Kui kontekstist on selge, milliste mõõtmetega maatriksitega on tegu, võib maatriksite liitmise definitsiooni anda lühemal kujul:

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}).$$

Tabelite kujul näeb liitmisreegel välja nii:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{pmatrix},$$

s.t. *maatriksite liitmisel liidetakse nende vastavatel kohtadel olevad elemendid.* Rõhutame veelkord, et liita saab vaid samade mõõtmetega maatrikseid.

Liitmise ja vastandmaatriksi abil saab defineerida maatriksite lahutamise. **Maatriksite** $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ ja $B = (b_{ij}) \in \mathrm{Mat}_{m,n}$ **vahe** on maatriks

$$A - B := A + (-B).$$

Seega $A - B = (c_{ij}) \in \mathrm{Mat}_{m,n}$, kus $c_{ij} = a_{ij} + (-b_{ij}) = a_{ij} - b_{ij}$ iga $i \in \{1,\dots,m\}$ ja $j \in \{1,\dots,n\}$ korral.

Definitsioon 1.22 Maatriksi $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ **ja arvu** $k \in \mathbb{R}$ **korrutis** on maatriks $kA = (c_{ij}) \in \mathrm{Mat}_{m,n}$, kus $c_{ij} = ka_{ij}$ iga $i \in \{1,\dots,m\}$ ja $j \in \{1,\dots,n\}$ korral.

Seega

$$k(a_{ij}) = (ka_{ij})$$

ehk

$$k \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} ka_{11} & ka_{12} & \dots & ka_{1n} \\ ka_{21} & ka_{22} & \dots & ka_{2n} \\ \dots & \dots & \dots & \dots \\ ka_{m1} & ka_{m2} & \dots & ka_{mn} \end{pmatrix},$$

s.t. *maatriksi korrutamisel arvuga k korrutatakse selle maatriksi kõik elemendid arvuga k.* Muuhulgas

$$(-1)A = -A.$$

[1] Leopold Kronecker (1823–1891) — saksa matemaatik

Näide 1.23 Näiteks

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 1 & -2 & -2 & 1 \\ -2 & -3 & -1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 & 5 \\ 2 & 0 & 1 & 5 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} - \begin{pmatrix} 1 & -2 & -2 & 1 \\ -2 & -3 & -1 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 4 & 5 & 3 \\ 6 & 6 & 3 & -3 \end{pmatrix},$$

$$3 \cdot \begin{pmatrix} 2 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 6 & 3 \\ 0 & -3 \end{pmatrix}.$$

Defineeritud tehetel on terve rida häid omadusi.

Lause 1.24 *Mistahes $A, B, C \in \mathrm{Mat}_{m,n}$ ja $k, l \in \mathbb{R}$ korral*

1. $(A + B) + C = A + (B + C)$;
2. $A + \Theta_{m,n} = A = \Theta_{m,n} + A$;
3. $A + (-A) = \Theta_{m,n} = (-A) + A$;
4. $A + B = B + A$;
5. $k(A + B) = kA + kB$;
6. $(k + l)A = kA + lA$;
7. $(kl)A = k(lA)$;
8. $1A = A$.

Tõestus. 1. Olgu $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}) \in \mathrm{Mat}_{m,n}$. Siis

$$\begin{aligned} (A + B) + C &= ((a_{ij}) + (b_{ij})) + (c_{ij}) \underset{\text{Def. 1.21}}{=} (a_{ij} + b_{ij}) + (c_{ij}) \underset{\text{Def. 1.21}}{=} ((a_{ij} + b_{ij}) + c_{ij}) \\ &\underset{\text{RA1}}{=} (a_{ij} + (b_{ij} + c_{ij})) \underset{\text{Def. 1.21}}{=} (a_{ij}) + (b_{ij} + c_{ij}) \underset{\text{Def. 1.21}}{=} (a_{ij}) + ((b_{ij}) + (c_{ij})) \\ &= A + (B + C). \end{aligned}$$

2. Olgu $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ ja vaatleme $(m \times n)$-nullmaatriksit $\Theta_{m,n} = (\theta_{ij})$, kus $\theta_{ij} = 0$ iga i ja j korral. Siis

$$A + \Theta_{m,n} = (a_{ij}) + (\theta_{ij}) \underset{\text{Def. 1.21}}{=} (a_{ij} + \theta_{ij}) = (a_{ij} + 0) \underset{RA2}{=} (a_{ij}) = A.$$

Teise võrduse saab tõestada anaoogiliselt.

5. Olgu $A = (a_{ij}), B = (b_{ij}) \in \mathrm{Mat}_{m,n}$ ja $k \in \mathbb{R}$. Siis

$$\begin{aligned} k(A + B) &= k((a_{ij}) + (b_{ij})) \underset{\text{Def. 1.21}}{=} k(a_{ij} + b_{ij}) \underset{\text{Def. 1.22}}{=} (k(a_{ij} + b_{ij})) \\ &\underset{RA7}{=} (ka_{ij} + kb_{ij}) \underset{\text{Def. 1.21}}{=} (ka_{ij}) + (kb_{ij}) \underset{\text{Def. 1.22}}{=} k(a_{ij}) + k(b_{ij}) = kA + kB. \end{aligned}$$

Nagu näeme, on omaduste 1, 2 ja 5 tõestamiseks vaja kasutada vaid maatriksite liitmise ja arvuga korrutamise definitsiooni ning reaalarvude omadusi. Ka ülejäänud väidete tõestamine taandub tehete definitsioonide ja reaalarvude omaduste kasutamisele. Need tõestused jätame läbi mõtlemiseks lugejale. □

1.5 Maatriksite korrutamine

Maatriksite korrutise definitsioon on mõnevõrra keerulisem kui maatriksite summa definitsioon. Kahte maatriksit saab korrutada ainult siis, kui esimese maatriksi veergude arv on võrdne teise maatriksi ridade arvuga.

Definitsioon 1.25 Maatriksite $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ ja $B = (b_{ij}) \in \mathrm{Mat}_{n,p}$ **korrutiseks** nimetatakse maatriksit $C = (c_{ij}) \in \mathrm{Mat}_{m,p}$, kus iga $i \in \{1, \ldots, m\}$ ja $j \in \{1, \ldots, p\}$ korral

$$\boxed{c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}.}$$

Niisiis *selleks, et leida korrutise C element, mis asub i-ndas reas ja j-ndas veerus, tuleb maatriksi A i-nda rea elemendid korrutada maatriksi B j-nda veeru vastavate elementidega ja tulemused liita.*

Harilikult kirjutatakse korrutise C asemel AB.

Näide 1.26 Näiteks

$$\begin{pmatrix} 1 & 3 & 1 \\ 0 & -2 & 4 \end{pmatrix} \begin{pmatrix} 2 & -3 \\ 1 & 2 \\ 5 & -1 \end{pmatrix} = \begin{pmatrix} 2+3+5 & -3+6-1 \\ 0-2+20 & 0-4-4 \end{pmatrix} = \begin{pmatrix} 10 & 2 \\ 18 & -8 \end{pmatrix},$$

$$\begin{pmatrix} 2 & -3 \\ 1 & 2 \\ 5 & -1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 1 \\ 0 & -2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 12 & -10 \\ 1 & -1 & 9 \\ 5 & 17 & 1 \end{pmatrix}.$$

Definitsioonist on kohe selge, et leidub maatrikseid, mille korral korrutis AB on olemas, aga korrutist BA ei leidu. Isegi siis, kui AB ja BA leiduvad, ei pruugi nad võrdsed olla, nagu näha eelnenud näitest. Seega maatriksite korrutamine ei ole kommutatiivne. Siiski on maatriksite korrutamisel rida omadusi, mis on sarnased reaalarvude korrutamise omadustega.

Lause 1.27 *Maatriksite korrutamisel on järgmised omadused.*

1. *Mistahes $A \in \mathrm{Mat}_{m,n}$, $B \in \mathrm{Mat}_{n,p}$ ja $C \in \mathrm{Mat}_{p,q}$ korral*

$$(AB)C = A(BC).$$

2. *Mistahes $A \in \mathrm{Mat}_{m,n}$ korral*

$$E_m A = A \quad \text{ja} \quad AE_n = A,$$

kus $E_m \in \mathrm{Mat}_m$ ja $E_n \in \mathrm{Mat}_n$ on vastavat järku ühikmaatriksid.

3. *Mistahes $A, B \in \mathrm{Mat}_{m,n}$, $C \in \mathrm{Mat}_{n,p}$ korral*

$$(A + B)C = AC + BC.$$

4. *Mistahes $A \in \mathrm{Mat}_{m,n}$, $B, C \in \mathrm{Mat}_{n,p}$ korral*

$$A(B + C) = AB + AC.$$

5. *Mistahes* $A \in \mathrm{Mat}_{m,n}$, $B \in \mathrm{Mat}_{n,p}$ *ja* $k \in \mathbb{R}$ *korral*

$$k(AB) = (kA)B = A(kB).$$

6. *Mistahes* $A \in \mathrm{Mat}_{m,n}$ *ja* $p, q \in \mathbb{N}$ *korral*

$$\Theta_{q,m}A = \Theta_{q,n} \quad ja \quad A\Theta_{n,p} = \Theta_{m,p}.$$

Tõestus. 1. Olgu $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$, $B = (b_{ij}) \in \mathrm{Mat}_{n,p}$ ja $C = (c_{ij}) \in \mathrm{Mat}_{p,q}$. Toome sisse tähised maatriksite $AB, (AB)C, BC$ ja $A(BC)$ elementide jaoks:

$$\begin{aligned} AB &= (u_{ij}) \in \mathrm{Mat}_{m,p}, \\ (AB)C &= (v_{ij}) \in \mathrm{Mat}_{m,q}, \\ BC &= (w_{ij}) \in \mathrm{Mat}_{n,q}, \\ A(BC) &= (t_{ij}) \in \mathrm{Mat}_{m,q}. \end{aligned}$$

Kasutades maatriksite korrutamise definitsiooni, summeerimise omadusi ja reaalarvude korrutamise assotsiatiivsust võime kirjutada:

$$u_{ik} \underset{\text{Def. 1.25}}{=} \sum_{l=1}^{n} a_{il}b_{lk},$$

$$v_{ij} \underset{\text{Def. 1.25}}{=} \sum_{k=1}^{p} u_{ik}c_{kj} = \sum_{k=1}^{p} \left(\sum_{l=1}^{n} a_{il}b_{lk} \right) c_{kj} \underset{SO1}{=} \sum_{k=1}^{p} \sum_{l=1}^{n} (a_{il}b_{lk})\, c_{kj} \underset{RA5}{=} \sum_{k=1}^{p} \sum_{l=1}^{n} a_{il}(b_{lk}c_{kj}),$$

$$w_{lj} \underset{\text{Def. 1.25}}{=} \sum_{k=1}^{p} b_{lk}c_{kj},$$

$$t_{ij} \underset{\text{Def. 1.25}}{=} \sum_{l=1}^{n} a_{il}w_{lj} = \sum_{l=1}^{n} a_{il} \left(\sum_{k=1}^{p} b_{lk}c_{kj} \right) \underset{SO1}{=} \sum_{l=1}^{n} \sum_{k=1}^{p} a_{il} \left(b_{lk}c_{kj} \right) \underset{SO3}{=} \sum_{k=1}^{p} \sum_{l=1}^{n} a_{il} \left(b_{lk}c_{kj} \right).$$

Kuna $v_{ij} = t_{ij}$ iga $i \in \{1, \ldots, m\}$ ja $j \in \{1, \ldots, q\}$ korral, siis on maatriksid $(AB)C$ ja $A(BC)$ võrdsed, $(AB)C = A(BC)$.

2. Olgu $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ ja olgu $E_m = (\delta_{ij})$ m-ndat järku ühikmaatriks. Siis korrutise $E_mA \in \mathrm{Mat}_{m,n}$ i-ndas reas ja j-ndas veerus on arv

$$\sum_{k=1}^{m} \delta_{ik}a_{kj} = \delta_{i1}a_{1j} + \delta_{i2}a_{2j} + \ldots + \delta_{im}a_{mj} = \delta_{ii}a_{ij} = 1 \cdot a_{ij} = a_{ij}.$$

Järelikult $E_mA = A$, sest nende maatriksite vastavatel kohtadel olevad elemendid on võrdsed. Võrduse $AE_n = A$ saab tõestada analoogiliselt.

3. Olgu $A = (a_{ij}), B = (b_{ij}) \in \mathrm{Mat}_{m,n}$, $C = (c_{ij}) \in \mathrm{Mat}_{n,p}$. Toome sisse tähised maatriksite $(A + B)C, AC$ ja BC elementide jaoks:

$$\begin{aligned} (A+B)C &= (u_{ij}) \in \mathrm{Mat}_{m,p}, \\ AC &= (v_{ij}) \in \mathrm{Mat}_{m,p}, \\ BC &= (w_{ij}) \in \mathrm{Mat}_{m,p}. \end{aligned}$$

Et maatriksis $A + B$ kohal (i, k) on element $a_{ik} + b_{ik}$, siis

$$u_{ij} \underset{\text{Def.1.25}}{=} \sum_{k=1}^{n} (a_{ik} + b_{ik})c_{kj} \underset{RA7}{=} \sum_{k=1}^{n} (a_{ik}c_{kj} + b_{ik}c_{kj}) \underset{SO2}{=} \sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj} \underset{\text{Def.1.25}}{=} v_{ij} + w_{ij}$$

iga $i \in \{1, \ldots, m\}$ ja $j \in \{1, \ldots, p\}$ korral. Kuna maatriksites $(A+B)C$ ja $AC+BC$ on vastavatel kohtadel samad elemendid, siis on need maatriksid võrdsed.

Ülejäänud omadused saab tõestada analoogiliselt. □

1.6 Transponeerimise omadused

Uurime nüüd, kuidas on transponeerimine seotud maatriksite liitmisega, maatriksi arvuga korrutamisega ja maatriksite korrutamisega.

Lause 1.28 *Maatriksite transponeerimisel on järgmised omadused.*

1. *Mistahes* $A, B \in \mathrm{Mat}_{m,n}$ *korral*

$$(A + B)^T = A^T + B^T.$$

2. *Mistahes* $A \in \mathrm{Mat}_{m,n}$ *ja* $k \in \mathbb{R}$ *korral*

$$(kA)^T = kA^T.$$

3. *Mistahes* $A \in \mathrm{Mat}_{m,n}$ *ja* $B \in \mathrm{Mat}_{n,p}$ *korral*

$$(AB)^T = B^T A^T.$$

TÕESTUS. Tõestame neist omadustest viimase (ülejäänud jäävad jälle lugejale läbi mõtlemiseks). Olgu $A = (a_{ij}) \in \mathrm{Mat}_{m,n}$ ja $B = (b_{ij}) \in \mathrm{Mat}_{n,p}$. Paneme tähele, et $B^T \in \mathrm{Mat}_{p,n}$ ja $A^T \in \mathrm{Mat}_{n,m}$, seega on korrutis $B^T A^T$ olemas ja $B^T A^T$ on $(p \times m)$-maatriks, nagu ka $(AB)^T$. Maatriksi $(AB)^T$ i-ndas reas ja j-ndas veerus on maatriksi AB j-nda rea ja i-nda veeru element, s.o. arv

$$\sum_{k=1}^{n} a_{jk} b_{ki}.$$

Maatriksi $B^T A^T$ i-ndas reas ja j-ndas veerus on element

$$\sum_{k=1}^{n} u_{ik} v_{kj},$$

kus u_{ik} on B^T i-nda rea ja k-nda veeru element ja v_{kj} on A^T k-nda rea ja j-nda veeru element. Maatriksi transponeerimise definitsiooni kohaselt $u_{ik} = b_{ki}$ ja $v_{kj} = a_{jk}$. Seega

$$\sum_{k=1}^{n} u_{ik} v_{kj} = \sum_{k=1}^{n} b_{ki} a_{jk} = \sum_{k=1}^{n} a_{jk} b_{ki}.$$

Järelikult kehtib võrdus $(AB)^T = B^T A^T$. □

2 Determinandid

2.1 Sissejuhatus

Vaatleme jälle lihtsat lineaarvõrrandisüsteemi

$$\begin{cases} a_{11}x_1 & + & a_{12}x_2 & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & = & b_2 \end{cases}, \tag{5}$$

milles on kaks tundmatut ja kaks võrrandit. Korrutades teise võrrandi $-a_{12}$-ga ja liites sellele esimese võrrandi, mis on korrutatud a_{22}-ga saame ühe tundmatuga lineaarvõrrandi

$$(a_{11}a_{22} - a_{12}a_{21})x_1 = b_1a_{22} - a_{12}b_2.$$

Teisest küljest, korrutades esimest võrrandit $-a_{21}$-ga ja liites sellele a_{11}-ga korrutatud teise võrrandi saame

$$(a_{11}a_{22} - a_{12}a_{21})x_2 = a_{11}b_2 - b_1a_{21}.$$

Kui nüüd $a_{11}a_{22} - a_{12}a_{21} \neq 0$, siis on süsteemil (5) täpselt üks lahend

$$x_1 = \frac{b_1a_{22} - a_{12}b_2}{a_{11}a_{22} - a_{12}a_{21}}, \qquad x_2 = \frac{a_{11}b_2 - b_1a_{21}}{a_{11}a_{22} - a_{12}a_{21}}. \tag{6}$$

Tuues sisse tähistuse

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} := ad - bc \tag{7}$$

võime valemid (6) esitada kujul

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, \qquad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}. \tag{8}$$

Kirjapilt (7) viitab sellele, et me tahame arvu $ad-bc$ siduda maatriksiga $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Tõepoolest, arvu $ad - bc$ nimetatakse teist järku ruutmaatriksi $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ **determinandiks**. Valemid (8) näitavad, et teatud tüüpi lineaarvõrrandisüsteeme saab lahendada selliste teist järku ruutmaatriksite determinantide abil, mille veergudes on tundmatute kordajad ja vabaliikmed. Osutub, et on võimalik defineerida ka n-ndat järku ruutmaatriksite determinandid ja nende abil lahendada teatud n tundmatu ja n võrrandiga lineaarvõrrandisüsteeme. Kui teist järku ruutmaatriksi determinant on kahe korrutise summa $(ad + (-bc))$, siis n-ndat järku ruutmaatriksi determinant on $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ liidetava summa. Et seda defineerida, peame enne tutvuma permutatsiooni ja substitutsiooni mõistega.

2.2 Substitutsioonid

Definitsioon 2.1 Olgu n naturaalarv ja olgu A n-elemendiline hulk. **Permutatsioon** hulga A elementidest on selline n-elemendiline järjestatud jada, milles hulga A iga element esineb täpselt ühe korra.

Enamasti vaadeldakse matemaatikas permutatsioone hulga $A = \{1, 2, \ldots, n\}$ elementidest ja öeldakse, et need on **permutatsioonid** n **elemendist**. Sellist permutatsiooni tähistame $(i_1, i_2, \ldots, i_n)$. Tihti kirjutatakse ka lihtsalt $i_1 i_2 \ldots i_n$ (näiteks raamatus [1]). Lihtne on aru saada, et permutatsioone n elemendist on $n!$ tükki.

Näiteks $(4, 1, 3, 5, 2)$ on permutatsioon 5-st elemendist, aga $(4, 1, 3, 4, 2)$ ja $(2, 5, 4, 3)$ ei ole.

Definitsioon 2.2 Permutatsiooni $(1, 2, \ldots, n)$ nimetatakse **loomulikuks permutatsiooniks** n elemendist.

Definitsioon 2.3 Öeldakse, et üks permutatsioon on saadud teisest **transpositsiooni** abil, kui see esimene permutatsioon on saadud teisest kahe elemendi äravahetamise teel.

Näiteks permutatsioon $(4, 1, 3, 5, 2)$ on saadud permutatsioonist $(4, 1, 2, 5, 3)$ kolmanda ja viienda elemendi äravahetamise teel.

Lause 2.4 *Kõik permutatsioonid n elemendist on võimalik niiviisi järjestada, et iga järgnev permutatsioon on eelnevast saadav transpositsiooni abil, kusjuures esimeseks võib valida suvalise permutatsiooni.*

Tõestus. Tõestame lause matemaatilise induktsiooniga elementide arvu n järgi. Kui $n = 1$, siis on väide ilmne. Kui $n = 2$ ja esimene permutatsioon on (i_1, i_2), siis teine permutatsioon (i_2, i_1) on esimesest saadav transpositsiooni abil. Rohkem permutatsioone 2-st elemendist pole. Oletame nüüd, et $n \geqslant 3$ ja lause väide kehtib permutatsioonide jaoks $n-1$ elemendist. Võtame suvalise permutatsiooni

$$(i_1, i_2, i_3, \ldots, i_n)$$

n elemendist. Vaatleme kõiki permutatsioone n elemendist, mis algavad elemendiga i_1. Kui neist esimene komponent i_1 ära jätta, siis saame kõik permutatsioonid $n-1$ elemendist $i_2, \ldots, i_n$. Induktsiooni eelduse põhjal võime need järjestada sellisel viisil, et iga järgnev on saadud eelnevast transpositsiooni abil. Olgu sellise järjestuse viimane permutatsioon

$$(i_1, j_2, j_3, \ldots, j_n).$$

Transpositsiooni abil, mis vahetab ära i_1 ja j_2 saame permutatsiooni

$$(j_2, i_1, j_3, \ldots, j_n).$$

Järjestame nüüd nõutaval viisil kõik permutatsioonid elementidest $i_1, j_3, \ldots, j_n$. Lisades neile ette j_2 saame vajaliku järjestuse kõigi permutatsioonide jaoks, mille esimene komponent on j_2. Olgu selles järjestuses viimane permutatsioon

$$(j_2, k_2, k_3, \ldots, k_n).$$

Leiame elementide $k_2, k_3, \ldots, k_n$ hulgast sellise elemendi k_s, mis ei kuulu hulka $\{i_1, j_2\}$. Vahetame ära j_2 ja k_s (s.t. teeme transpositsiooni) ja järjestame nõutaval viisil kõik permutatsioonid, mille esimene komponent on k_s. Nii jätkates saame nõutaval viisil ära järjestada kõik permutatsioonid, mille esimene komponent on $1, 2, \ldots, n$, s.t. kõikvõimalikud permutatsioonid elementidest $1, 2, \ldots, n$. □

Näide 2.5 Võttes esimeseks permutatsiooniks $(2, 1, 3)$ võime kõik 6 permutatsiooni kolmest elemendist lause tõestuses kasutatud meetodi abil järjestada nii:

$$(2, 1, 3),\ \ (2, 3, 1),\ \ (3, 2, 1),\ \ (3, 1, 2),\ \ (1, 3, 2),\ \ (1, 2, 3).$$

Definitsioon 2.6 Öeldakse, et elemendid i_k ja i_l moodustavad **inversiooni** permutatsioonis $(i_1, i_2, \ldots, i_k, \ldots, i_l, \ldots, i_n)$, kui $k < l$ ja $i_k > i_l$. Inversioonide koguarvu permutatsioonis $(i_1, i_2, \ldots, i_n)$ tähistame sümboliga $I(i_1, i_2, \ldots, i_n)$.

Permutatsiooni nimetatakse **paarispermutatsiooniks**, kui inversioonide koguarv selles permutatsioonis on paarisarv. Vastasel juhul nimetatakse seda permutatsiooni **paarituks permutatsiooniks**.

Näide 2.7 Permutatsioonis $(4, 1, 3, 5, 2)$ moodustavad inversiooni elementide paarid $(4, 1)$, $(4, 3)$, $(4, 2)$, $(3, 2)$ ja $(5, 2)$. Seega inversioone on 5 tükki, $I(4, 1, 3, 5, 2) = 5$, ja tegemist on paaritu permutatsiooniga.

Permutatsioonis $(1, 2, 3, 4, 5)$ on aga 0 inversiooni ja seega on tegu paarispermutatsiooniga.

Lause 2.8 *Transpositsioon muudab permutatsiooni paarsust.*

Tõestus. Vaatleme esialgu juhtumit, kus permutatsioonis vahetatakse ära kõrvutiasetsevad elemendid i ja j. Sellise transpositsiooni käigus ei muutu nende inversioonide arv, mida i ja j moodustavad ülejäänud elementidega. Kui i ja j enne transpositsiooni ei moodustanud inversiooni, siis pärast transpositsiooni nad moodustavad, ja vastupidi. Seega inversioonide koguarv kas suureneb või väheneb ühe võrra ja sellega paarsus muutub.

Nüüd vaatleme olukorda, kus äravahetatavate elementide i ja j vahel on m elementi $i_1, \ldots, i_m$, s.t. et permutatsioon on kujul

$$(\ldots, i, i_1, \ldots, i_m, j, \ldots). \tag{9}$$

Sel juhul kujutame i ja j äravahetamist ette järgimselt. Vahetame ära i ja i_1, siis i ja i_2 jne., kuni vahetame ära i ja i_m ning seejärel i ja j. Siis vahetame ära j ja i_m, j ja i_{m-1}, jne. kuni on vahetatud j ja i_1. Tulemuseks on permutatsioon

$$(\ldots, j, i_1, \ldots, i_m, i, \ldots). \tag{10}$$

Seega näeme, et i-d ja j-i vahetava transpositsiooni saab esitada $2m + 1$ kõrvutiasetsevate elementide transpositsiooni järjestrakendamisena. Tõestuse esimese osa põhjal teame, et niimoodi muutub permutatsiooni paarsus $2m+1$ korda, mis aga tähendabki, et permutatsiooni (9) paarsus erineb permutatsiooni (10) paarsusest. □

Definitsioon 2.9 Substitutsiooniks lõplikul hulgal M nimetatakse hulga M bijektiivset teisendust, s.t. üksühest pealekujutust $M \to M$.

Märkus 2.10 Tihti (eriti ingliskeelses kirjanduses) kasutatakse ka lõpliku hulga bijektiivsetest teisendustest rääkides sõna "permutatsioon". Selles kursuses me üritame sellist lähenemist vältida.

Harilikult vaadeldakse substitutsioone hulgal $M = \{1, 2, \ldots, n\}$ ja kutsutakse neid **substitutsioonideks n elemendist**. Kõigi substitutsioonide hulka n-elemendist tähistatakse sümboliga S_n. Substitutsioone tähistatakse tavaliselt väikeste kreeka tähtedega $\sigma, \tau, \ldots$.

Substitutsiooni esitamiseks kasutatakse tihti 2-realist ja n-veerulist tabelit (s.o, $(2 \times n)$-maatriksit), mille esimeses reas on hulga $\{1, 2, \ldots, n\}$ elemendid mingis järjekorras ja teises reas on esimeses reas olevate elementide kujutised, seega

$$\sigma = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ \sigma(i_1) & \sigma(i_2) & \ldots & \sigma(i_n) \end{pmatrix}.$$

Nii sellise tabeli esimese rea kui ka teise rea elemendid moodustavad permutatsiooni.

Definitsioon 2.11 Substitutsiooni nimetatakse **paarissubstitutsiooniks**, kui inversioonide koguarv permutatsioonides tema esituses tabelina on paarisarv. Vastasel korral nimetatakse seda substitutsiooni **paarituks substitutsiooniks**.

Osutub, et see definitsioon on korrektne selles mõttes, et substitutsiooni paarsus ei sõltu tema esitusest tabelina. Selle näitamiseks oletame, et substitutsioon σ on esitatud kahel viisil:

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma(i_1) & \sigma(i_2) & \dots & \sigma(i_n) \end{pmatrix} = \begin{pmatrix} j_1 & j_2 & \dots & j_n \\ \sigma(j_1) & \sigma(j_2) & \dots & \sigma(j_n) \end{pmatrix}.$$

Kui vahetame tabelis ära kaks veergu, siis saame sama substitutsiooni uue esituse. Selle vahetuse käigus toimub nii ülemises kui alumises permutatsioonis transpositsioon, mis muudab kummagi permutatsiooni paarsust. Inversioonide koguarvu paarsus tabelis aga ei muutu. Järjestame nüüd permutatsioonid n elemendist lauses 2.4 kirjeldatud viisil nii, et alustame permutatsioonist $(i_1, i_2, \dots, i_n)$. Selles järjestuses peab esinema ka permutatsioon $(j_1, j_2, \dots, j_n)$. Tehes vastavad transpositsioonid tabeli veergudega saame esimesest tabelist teise, kusjuures inversioonide koguarvu paarsus ühegi sammu käigus ei muutu. See näitabki, et inversioonide koguarvu paarsus ei sõltu substitutsiooni esitusest tabelina.

Näide 2.12 Leiame substitutsiooni

$$\sigma = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix} \in S_4$$

paarsuse. Kuna $I(2,3,4,1) + I(3,4,1,2) = 3 + 4 = 7$ on paaritu arv, siis σ on paaritu substitutsioon.

Iga substitutsiooniga saab siduda tema "märgi" (+ või −). Täpsemalt öeldes võib vaadelda kujutust

$$\operatorname{sign} : \bigcup_{n \in \mathbb{N}} S_n \to \{1, -1\}$$

(ladinakeelsest sõnast *signum*, mis tähendab märki), mis on defineeritud võrdusega

$$\boxed{\operatorname{sign}(\sigma) := \begin{cases} 1, & \text{kui } \sigma \text{ on paarissubstitutsioon,} \\ -1, & \text{kui } \sigma \text{ on paaritu substitutsioon.} \end{cases}}$$

Kõige sagedamini esitatakse substitutsioon tabelina nii, et selle esimeses reas on loomulik permutatsioon $(1, 2, 3, \dots, n)$:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Sellist tabelit nimetatakse substitutsiooni σ **normaalkujuks**.

Tuletame meelde, et hulga M teisendusi on võimalik korrutada (s.t. järjest rakendada). Kui τ ja σ on hulga M teisendused, siis nende korrutis $\tau\sigma$ (vahel tähistatakse ka $\tau \circ \sigma$) on hulga M teisendus, mis on defineeritud eeskirjaga

$$\boxed{(\tau\sigma)(m) := \tau(\sigma(m))}$$

iga $m \in M$ korral. Seega saame korrutada ka substitutsioone.

Näide 2.13 Leiame substitutsioonide

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{ja} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

korrutise $\tau\sigma$. Kuna $(\tau\sigma)(1) = \tau(\sigma(1)) = \tau(2) = 4$, $(\tau\sigma)(2) = \tau(\sigma(2)) = \tau(3) = 3$, $(\tau\sigma)(3) = 1$ ja $(\tau\sigma)(4) = 2$, siis

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Samasusteisendust 1_M nimetame hulga M **ühiksubstitutsiooniks** ja tähistame sümboliga ε (kreeka täht epsilon). Seega kui $M = \{1, 2, \ldots, n\}$, siis

$$\varepsilon = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Hulgateooriast teame, et hulga M igal bijektiivsel teisendusel σ on olemas pöördteisendus, s.t. teisendus σ^{-1}, mis rahuldab seoseid $\sigma\sigma^{-1} = 1_M$ ja $\sigma^{-1}\sigma = 1_M$. Substitutsiooni $\sigma \in S_n$ pöördteisendust nimetatakse σ **pöördsubstitutsiooniks** ja tähistatakse sümboliga σ^{-1}. On selge, et kui

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}, \tag{11}$$

siis

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \ldots & \sigma(n) \\ 1 & 2 & \ldots & n \end{pmatrix}, \tag{12}$$

s.t. pöördsubstitutsiooni saamiseks võib σ esituses tabelina read ära vahetada.

Näide 2.14 Kui

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

siis

$$\sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Lause 2.15 *Substitutsioon ja tema pöördsubstitutsioon on sama paarsusega.*

Tõestus. Inversioonide koguarv tabelites (11) ja (12) on sama. □

2.3 Determinandi definitsioon

Seome nüüd iga ruutmaatriksiga teatud arvu.

Definitsioon 2.16 Ruutmaatriksi

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

determinandiks nimetatakse reaalarvu, mida tähistatakse

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

(või $\det(A)$) ja mis defineeritakse kui summa

$$\boxed{|A| := \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}.} \tag{13}$$

n-ndat järku ruutmaatriksi determinanti nimetatakse **n-ndat järku determinandiks**. Korrutisi $a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}$ nimetatakse **determinandi $|A|$ liikmeteks**.

Kommenteerime pisut seda definitsiooni. Selles summas liidetakse märgiga ($\operatorname{sign}(\sigma)$) varustatud korrutisi n-st maatriksi A elemendist, kusjuures korrutises on igast reast ja igast veerust üks tegur. Seda, et igast veerust on võetud täpselt üks tegur, näitab see, et elementide veeruindeksid moodustavad permutatsiooni $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Kuna permutatsioonis $(1, 2, \ldots, n)$ on 0 inversiooni, siis korrutise $a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}$ märk on $+$ siis, kui $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ on paarispermutatsioon ja $-$ vastasel juhul. Summeerimine toimub üle kõigi substitutsioonide hulgal $\{1, 2, \ldots, n\}$, s.t. liita tuleb kõikvõimalikud sellised korrutised.

Definitsiooni põhjal on lihtne veenduda, et kui $A = (a) \in \mathrm{Mat}_1$, siis $|A| = a$, ja et

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Kuna $|S_n| = n!$, siis definitsiooni järgi arvutades tuleb näiteks 4-ndat järku determinandi puhul liita $4! = 24$ korrutist, 5-ndat järku determinandi puhul $5! = 120$ korrutist jne. On selge, et vähegi suurema järgu korral on determinandi arvutamine definitsiooni järgi väga töömahukas. Õnneks on determinandil mitmeid omadusi, mis tema arvutamist lihtsustavad. Vaatlemegi neid omadusi lähemalt.

2.4 Determinandi omadused

Teoreem 2.17 *Transponeerimisel maatriksi determinant ei muutu.*

Tõestus. Olgu $A = (a_{ij}) \in \mathrm{Mat}_n$. Me peame tõestama, et

$$\boxed{|A^T| = |A|.}$$

Definitsiooni põhjal

$$|A| = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)}. \tag{14}$$

ja

$$|A^T| = \sum_{\tau \in S_n} m_\tau, \tag{15}$$

kus m_τ on substitutsioonile τ vastav liidetav. Vaatleme $|A|$ suvalist liiget $a_{1\sigma(1)}a_{2\sigma(2)} \ldots a_{n\sigma(n)}$, mis vastab substitutsioonile

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Tegurid $a_{1\sigma(1)}$,$a_{2\sigma(2)}$,...,$a_{n\sigma(n)}$ kuuluvad maatriksi A^T ridadesse numbritega $\sigma(1), \sigma(2), \ldots, \sigma(n)$ ja veergudesse numbritega $1, 2, \ldots, n$. Seega on korrutis $a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}$ ka determinandi $|A^T|$ liige, kusjuures ta vastab substitutsioonile

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \ldots & \sigma(n) \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Lause 2.15 põhjal võime öelda, et kehtib võrdus $\text{sign}(\sigma) = \text{sign}(\sigma^{-1})$. Seega $\text{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot \ldots \cdot a_{n\sigma(n)} = m_{\sigma^{-1}}$, s.t. et iga liidetav summast (14) on ka liidetav summas (15). Kui oletada, et $\sigma^{-1} = \tau^{-1}$, kus $\sigma, \tau \in S_n$, siis $\sigma = (\sigma^{-1})^{-1} = (\tau^{-1})^{-1} = \tau$. Seega kui $\sigma \neq \tau$, siis $\sigma^{-1} \neq \tau^{-1}$. See tähendab, et erinevatele substitutsioonidele vastavad liidetavad summas (14) on võrdsed erinevatele substitutsioonidele vastavate liidetavatega summas (15). Kuna liidetavaid on mõlemas summas ühepalju, siis ongi need summad võrdsed ja $|A| = |A^T|$. □

Lause 2.18 *Kui ruutmaatriks sisaldab nullidest koosnevat rida, siis tema determinant on* 0.

Tõestus. Kui maatriksi $A = (a_{ij}) \in \text{Mat}_n$ k-s rida koosneb ainult nullidest, siis igas korrutises $a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}$ on k-s tegur võrdne nulliga ja seega on summa (13) kõik liidetavad nullid. □

Järeldus 2.19 *Kui ruutmaatriks sisaldab nullidest koosnevat veergu, siis tema determinant on* 0.

Tõestus. Kui ruutmaatriks A sisaldab nullidest koosnevat veergu, siis maatriks A^T sisaldab nullidest koosnevat rida. Lause 2.18 põhjal $|A^T| = 0$. Teoreemi 2.17 kasutades saame, et $|A| = |A^T| = 0$. □

Märkus 2.20 Edaspidi sõnastame ja tõestame veel terve rea determinantide omadusi ridade abil. Samasugused omadused saaks sõnastada ka veergude abil ja tõestada need Teoreemi 2.17 kasutades. Me ei hakka neid omadusi siin kirja panema ega tõestama, kuid vajaduse korral kasutame neid determinandi arvutamisel.

Lause 2.21 *Kui maatriksi mingi rea kõik elemendid korrutada arvuga c, siis tema determinant korrutub ka arvuga c.*

Tõestus. Olgu $A = (a_{ij}) \in \text{Mat}_n$ ja olgu B maatriks, mis on saadud maatriksist A k-nda rea korrutamisel arvuga c. Siis kasutades summeerimise omadust SO1 saame, et

$$\begin{aligned} |B| &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{k-1,\sigma(k-1)} \cdot ca_{k\sigma(k)} \cdot a_{k+1,\sigma(k+1)} \cdot \ldots \cdot a_{n\sigma(n)} \\ &= c\left(\sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}\right) = c \cdot |A|. \end{aligned}$$

□

Näide 2.22 Kui maatriksi

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}$$

teine rida korrutada arvuga 3, siis saadava maatriksi determinant on $3 \cdot |A|$:

$$\begin{vmatrix} 2 & 0 & 1 \\ 3 & 6 & -3 \\ 1 & 3 & 1 \end{vmatrix} = 3 \cdot \begin{vmatrix} 2 & 0 & 1 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{vmatrix}.$$

Lause 2.23 *Kui maatriksis vahetada ära kaks rida, siis determinant muudab märki.*

Tõestus. Olgu $A = (a_{ij}) \in \mathrm{Mat}_n$ ja olgu B maatriks, mis on saadud maatriksist A k-nda ja l-nda rea äravahetamisel, kus $k < l$, $k, l \in \{1, \ldots, n\}$. Definitsiooni põhjal

$$|A| = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k\sigma(k)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)}, \tag{16}$$

$$|B| = \sum_{\tau \in S_n} \mathrm{sign}(\tau) a_{1\tau(1)} \ldots a_{l\tau(k)} \ldots a_{k\tau(l)} \ldots a_{n\tau(n)}. \tag{17}$$

Peame näitama, et $|B| = -|A|$. Selleks vaatleme liidetavat

$$m_\sigma = \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k\sigma(k)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)}$$

summast (16). Kuna reaalarvude korrutamine on kommutatiivne, siis korrutis

$$a_{1\sigma(1)} \ldots a_{k\sigma(k)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)} = a_{1\sigma(1)} \ldots a_{l\sigma(l)} \ldots a_{k\sigma(k)} \ldots a_{n\sigma(n)}$$

esineb ka summas (17) liidetavana, mis vastab substitutsioonile

$$\sigma' = \begin{pmatrix} 1 & \ldots & k & \ldots & l & \ldots & n \\ \sigma(1) & \ldots & \sigma(l) & \ldots & \sigma(k) & \ldots & \sigma(n) \end{pmatrix},$$

mille ülemine permutatsioon on loomulik permutatsioon ja alumine permuatsioon on saadud permutatsioonist $(\sigma(1), \ldots, \sigma(k), \ldots, \sigma(l), \ldots, \sigma(n))$ transpositsiooni abil, mis vahetab ära k-nda ja l-nda elemendi. Kuna transpositsioon muudab permutatsiooni paarsust (lause 2.8), siis $\mathrm{sign}(\sigma) = -\mathrm{sign}(\sigma')$. Seega summa (16) iga liidetava m_σ, $\sigma \in S_n$, korral on $-m_\sigma$ substitutsioonile σ' vastav liidetav summas (17). Kui $\sigma, \rho \in S_n$ on erinevad substitutsioonid, siis ka $\sigma', \rho' \in S_n$ on erinevad. Seega kujul $-m_\sigma$ saame kätte $n!$ summa (17) liidetavat, mis vastavad erinevatele substitutsioonidele σ', s.t. me saame kätte kõik summa (17) liidetavad. Järelikult

$$|B| = \sum_{\sigma \in S_n} (-m_\sigma) = -\sum_{\sigma \in S_n} m_\sigma = -|A|.$$

□

Lause 2.24 *Kui ruutmaatriksis on kaks võrdset rida, siis tema determinant on* 0.

Tõestus. Olgu A maatriks, mille k-s ja l-s rida on võrdsed. Nende ridade äravahetamisel saame jälle maatriksi A ja lause 2.23 tõttu $|A| = -|A|$. Järelikult $2 \cdot |A| = 0$, millest saame võrduse $|A| = 0$. □

Järgmises lauses mõtleme maatriksi rea arvuga c korrutamise all seda, et selle rea kõik elemendid korrutatakse arvuga c, ja ridade liitmise all mõeldakse seda, et omavahel liidetakse nende ridade vastavad elemendid. Näiteks maatriksi

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ -2 & -4 & -5 \end{pmatrix}$$

kolmandale reale arvuga 2 korrutatud esimese rea liitmisel saame maatriksi

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Lause 2.25 *Kui ruutmaatriksi mingile reale liita suvalise arvuga korrutatud teine rida, siis selle maatriksi determinant ei muutu.*

TÕESTUS. Olgu $A = (a_{ij}) \in \mathrm{Mat}_n$ ja olgu B maatriks, mis on saadud maatriksist A selle k-ndale reale arvuga c korrutatud l-nda rea liitmisel, kus $k \neq l$. Peame näitama, et $|A| = |B|$.

Eeldame, et $k < l$. (Kui $k > l$, siis on tõestus analoogiline.) Maatriksi B k-s rida koosneb elementidest

$$a_{k1} + ca_{l1},\ a_{k2} + ca_{l2},\ \ldots\ , a_{kn} + ca_{ln};$$

kõik ülejäänud B elemendid on samad, mis A vastaval kohal olevad elemendid. Seega

$$|B| = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k-1,\sigma(k-1)} (a_{k\sigma(k)} + ca_{l\sigma(k)}) a_{k+1,\sigma(k+1)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)}.$$

Kasutades reaalarvude distributiivsuse ja summeerimise omadusi võime kirjutada

$$\begin{aligned} |B| &= \sum_{\sigma \in S_n} \big(\mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k-1,\sigma(k-1)} a_{k\sigma(k)} a_{k+1,\sigma(k+1)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)} \\ &\quad + \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k-1,\sigma(k-1)} (ca_{l\sigma(k)}) a_{k+1,\sigma(k+1)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)} \big) \\ &= \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k-1,\sigma(k-1)} a_{k\sigma(k)} a_{k+1,\sigma(k+1)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)} \\ &+ c \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \ldots a_{k-1,\sigma(k-1)} a_{l\sigma(k)} a_{k+1,\sigma(k+1)} \ldots a_{l\sigma(l)} \ldots a_{n\sigma(n)} \\ &= |A| + c \cdot 0 = |A|, \end{aligned}$$

kus eelviimases reas olev summa on 0 sellepärast, et ta on sellise maatriksi

$$A' = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k-1,1} & a_{k-1,2} & \ldots & a_{k-1,n} \\ a_{l1} & a_{l2} & \ldots & a_{ln} \\ a_{k+1,1} & a_{k+1,2} & \ldots & a_{k+1,n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{l1} & a_{l2} & \ldots & a_{ln} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

determinant, milles k-s ja l-s rida on võrdsed. □

Lause 2.25 on väga kasulik. Selle (ja tema analoogi) abil saame ridu või veerge omavahel liita nii, et tekiks juurde nulliga võrduvaid elemente, aga determinant samal ajal ei muutu. Mida rohkem on maatriksis nulle, seda lihtsam on leida tema determinandi väärtust. Kui näiteks õnnestub nullideks muuta kõik peadiagonaalist allpool olevad elemendid, siis piisab determinandi arvutamiseks vaid ühe korrutise leidmisest.

Maatriksit nimetatakse **ülemiseks kolmnurkmaatriksiks**, kui tema peadiagonaalist allpool asuvad elemendid on nullid.

Lause 2.26 *Ülemise kolmnurkmaatriksi*

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

determinant on

$$|A| = a_{11}a_{22}a_{33}\dots a_{nn}.$$

Tõestus. Definitsiooni põhjal tuleb determinandi leidmiseks liita korrutisi, kus igast reast ja veerust on võetud täpselt üks element. Kõik korrutised, kus tegurina esimesest veerust esineb 0, on võrdsed nulliga. Seega on mõtet vaadelda vaid korrutisi, kus esimese veeru esindaja on a_{11}. Kui teisest veerust tuleb 0, siis jällegi on korrutis 0. Element a_{12} teisest veerust tulla ei saa (sest siis oleks korrutises kaks elementi esimesest reast). Seega on mõtet vaadelda vaid korrutisi, kus on teguriteks a_{11} ja a_{22}. Analoogiliselt jätkates näeme, et ainuke korrutis, mis võib (aga ei pruugi) olla nullist erinev, on $a_{11}a_{22}a_{33}\dots a_{nn}$. See korrutis on määratud ühiksubstitusiooni poolt, järelikult on tema märk determinandi avaldises pluss. □

2.5 Laplace'i teoreem

Selle paragrahvi eesmärk on sõnastada Laplace'i[2] teoreem, mis lubab n-ndat järku determinandi arvutamise taandada madalamat järku determinantide arvutamisele. Teoreemi sõnastamiseks on meil vaja miinori mõistet.

Definitsioon 2.27 Maatriksi A **alammaatriksiks** nimetatakse maatriksit, mis saadakse, kui maatriksis A valitakse välja mingid read ja veerud ning moodustatakse uus maatriks elementidest, mis asuvad väljavalitud ridade ja veergude lõikekohtades, kusjuures nende elementide omavahelist asendit ei muudeta. **Alamruutmaatriks** on alammaatriks, milles on sama arv ridu ja veerge.

Definitsioon 2.28 Maatriksi A **k-ndat järku miinor** on tema k-ndat järku alamruutmaatriksi determinant.

Kui miinor on sellise alamruutmaatriksi determinant, mis on saadud ridade $i_1, \dots, i_k$ ja veergude $j_1, \dots, j_k$ väljavalimisel, siis ütleme, et see *miinor asub ridades $i_1, \dots, i_k$ ja veergudes $j_1, \dots, j_k$*.

Definitsioon 2.29 Kui ruutmaatriksi A miinor M asub ridades $i_1, \dots, i_k$ ja veergudes $j_1, \dots, j_k$, siis selle miinori **täiendusmiinoriks** nimetatakse miinorit $\tilde{M}$, mis asub ridades ja veergudes, mis jäävad järele ridade $i_1, \dots, i_k$ ja veergude $j_1, \dots, j_k$ väljajätmisel maatriksist A. Arvu

$$(-1)^{i_1+\dots+i_k+j_1+\dots+j_k}\tilde{M}$$

nimetatakse miinori M **algebraliseks täiendiks**.

Kui me tahame rõhutada, et vaadeldav miinor asub ridades $i_1, \dots, i_k$ ja veergudes $j_1, \dots, j_k$, siis kasutame selle miinori, tema täiendusmiinori ja algebralise täiendi jaoks järgmisi tähistusi:

$$M^{j_1,\dots,j_k}_{i_1,\dots,i_k}, \quad \tilde{M}^{j_1,\dots,j_k}_{i_1,\dots,i_k}, \quad A^{j_1,\dots,j_k}_{i_1,\dots,i_k}.$$

[2] Pierre-Simon Laplace (1749–1827) — prantsuse matemaatik.

Näide 2.30 Kui maatriksis

$$A = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}$$

valime välja read numbritega 2 ja 4 ning veerud numbritega 1 ja 4, siis saame, et

$$\begin{aligned} M_{2,4}^{1,4} &= \begin{vmatrix} e & h \\ m & p \end{vmatrix} = ep - hm, \\ \tilde{M}_{2,4}^{1,4} &= \begin{vmatrix} b & c \\ j & k \end{vmatrix} = bk - cj, \\ A_{2,4}^{1,4} &= (-1)^{2+4+1+4} \cdot \tilde{M}_{2,4}^{1,4} = -(bk - cj) = cj - bk. \end{aligned}$$

Järgneva teoreemi tõestas prantsuse matemaatik Pierre-Simon Laplace 1772. aastal. Meie toome selle siin ära ilma tõestuseta. Tõestuse võib leida näiteks raamatust [1].

Teoreem 2.31 (Laplace'i teoreem) *Olgu maatriksis $A \in \mathrm{Mat}_n$ fikseeritud read $i_1, \ldots, i_k$. Siis*

$$\boxed{|A| = \sum_{1 \leqslant j_1 < \ldots < j_k \leqslant n} M_{i_1,\ldots,i_k}^{j_1,\ldots,j_k} \cdot A_{i_1,\ldots,i_k}^{j_1,\ldots,j_k},}$$

s.t. A determinant on võrdne ridades $i_1, \ldots, i_k$ asuvate kõikvõimalike k-ndat järku miinorite ja nende miinorite algebraliste täiendite korrutiste summaga.

Kui Laplace'i teoreemi rakendatakse ridade $i_1, \ldots, i_k$ korral, siis räägitakse maatriksi A *determinandi arendamisest ridade $i_1, \ldots, i_k$ järgi.* Kuna transponeerimisel determinant ei muutu (vt. teoreemi 2.17), siis võib determinanti arendada ka veergude järgi.

Eriti kasulik on determinanti arendada mingite k rea järgi siis, kui neis ridades on ainult üks nullist erinev miinor. Sellisel juhul tuleb summasse ainult üks liidetav.

Näide 2.32 Järgneva determinandi kahes esimeses reas on ainult üks nullist erinev teist järku miinor (1. ja 3. veerus). Seega kahe esimese rea järgi arendades saame:

$$\begin{vmatrix} 1 & 0 & 2 & 0 \\ 3 & 0 & 4 & 0 \\ 9 & 5 & 10 & 6 \\ 11 & 7 & 12 & 8 \end{vmatrix} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \cdot (-1)^{1+2+1+3} \cdot \begin{vmatrix} 5 & 6 \\ 7 & 8 \end{vmatrix} = (-2) \cdot (-1) \cdot (-2) = -4.$$

Loomulikult võib determinanti arendada ka ühe rea või veeru järgi. Esimest järku miinor maatriksi A i-ndas reas ja j-ndas veerus on võrdne sellel kohal oleva arvuga a_{ij}. Sellise miinori algebralist täiendit tähistatakse A_i^j asemel harilikult sümboliga A_{ij}. Niisiis võime Laplace'i teoreemi põhjal öelda, et arendades i-nda rea järgi

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in} = \sum_{j=1}^{n} a_{ij}A_{ij} \qquad (18)$$

ja arendades j-nda veeru järgi

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = a_{1j}A_{1j} + a_{2j}A_{2j} + \ldots + a_{nj}A_{nj} = \sum_{i=1}^{n} a_{ij}A_{ij}.$$

Eelöeldut kokku võttes võib sõnastada järgmise meetodi n-ndat järku ruutmaatriksi A determinandi arvutamiseks.

1. Valime determinandis välja ühe rea või veeru (soovitavalt sellise, kus juba on nulle). Kui see rida või veerg koosneb ainult nullidest, siis $|A| = 0$. Vastasel korral võtame ühe nullist erineva elemendi ja muudame selle abil kõik ülejäänud elemendid antud reas või veerus nulliks kasutades liitmisteisendust. Determinant selle käigus ei muutu.

2. Arendame determinanti valitud rea või veeru järgi. Laplace'i teoreemi põhjal taandub $|A|$ arvutamine ühe $(n-1)$-st järku determinandi arvutamisele.

3. Kordame seda protseduuri kuni jõuame esimest järku determinandini.

2.6 Maatriksite korrutise determinant

Selles paragrahvis näitame, et determinandi leidmine on kooskõlas maatriksite korrutamisega.

Teoreem 2.33 *Sama järku ruutmaatriksite korrutise determinant on võrdne tegurite determinantide korrutisega.*

Tõestus. Olgu $A = (a_{ij}), B = (b_{ij}) \in \mathrm{Mat}_n$. Meie eesmärk on tõestada, et

$$\boxed{|AB| = |A| \cdot |B|.}$$

Vaatleme $2n$-järku determinanti

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 0 \\ -1 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1n} \\ 0 & -1 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix}.$$

Nagu näha, on D sellise maatriksi determinant, mis koosneb neljast nn. blokist: maatriksitest A, Θ, $-E$ ja B. Arendades seda determinanti D esimese n rea järgi näeme, et

$$D = |A| \cdot |B|,$$

sest $(1 + 2 + \ldots + n) + (1 + 2 + \ldots + n)$ on paarisarv. Teisendame nüüd seda determinanti nii, et kõik elemendid b_{ij} muutuksid nullideks. Selleks liidame $(n+1)$-sele veerule b_{11}-kordse

esimese veeru, b_{21}-kordse teise veeru jne., lõpuks b_{n1}-kordse n-nda veeru. Selle tulemusena ei jää $(n+1)$-se veeru esimesed n elementi enam nullideks, vaid omandavad uued väärtused

$$\begin{aligned} c_{11} &= a_{11}b_{11} + a_{12}b_{21} + \ldots + a_{1n}b_{n1}, \\ c_{21} &= a_{21}b_{11} + a_{22}b_{21} + \ldots + a_{2n}b_{n1}, \\ &\ldots \\ c_{n1} &= a_{n1}b_{11} + a_{n2}b_{21} + \ldots + a_{nn}b_{n1}. \end{aligned}$$

Teisendades analoogiliselt determinandis D ka ülejäänud elemendid b_{ij} nullideks saame determinandi

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} & c_{11} & c_{12} & \ldots & c_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} & c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} & c_{n1} & c_{n2} & \ldots & c_{nn} \\ -1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & -1 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & -1 & 0 & 0 & \ldots & 0 \end{vmatrix}, \tag{19}$$

kus

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Tähistades $C = (c_{ij}) \in \mathrm{Mat}_n$ näeme, et maatriks C on maatriksite A ja B korrutis, $AB = C$. Arendame nüüd determinanti D viimase n rea järgi kasutades selleks avaldist (19). Saame

$$D = (-1)^{1+2+\ldots+n+(n+1)+\ldots+2n} \cdot \begin{vmatrix} -1 & 0 & \ldots & 0 \\ 0 & -1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & -1 \end{vmatrix} \cdot |C| = (-1)^{1+2+\ldots+2n+n}|C| = |C|,$$

sest

$$1 + 2 + \ldots + 2n + n = \frac{(1+2n)2n}{2} + n = \frac{(2+2n)2n}{2} = 2n(n+1)$$

on paarisarv. □

3 Pöördmaatriks

Meenutame, et ühikmaatriks on ruutmaatriks, mille peadiagonaalil on ühed ja mille kõik muud elemendid on nullid:

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Teame, et reaalarv b on reaalarvu a pöördarv, kui $ab = ba = 1$. Analoogiliselt defineeritakse ka maatriksi pöördmaatriks.

Definitsioon 3.1 Maatriksi $A \in \mathrm{Mat}_n$ **pöördmaatriksiks** nimetatakse sellist maatriksit $B \in \mathrm{Mat}_n$, mille korral

$$AB = BA = E.$$

Maatriksit $A \in \mathrm{Mat}_n$ nimetatakse **pööratavaks**, kui tal leidub pöördmaatriks.

On selge, et mitte kõik ruutmaatriksid ei ole pööratavad. Näiteks nullmaatriksil puudub pöördmaatriks. Samas ühikmaatriks on alati pööratav, tema pöördmaatriks on ta ise, sest $EE = E$.

Lause 3.2 *Kui ruutmaatriksil leidub pöördmaatriks, siis on see üheselt määratud.*

Tõestus. Olgu B ja C maatriksi A pöördmaatriksid. Siis $AC = E$ ja $BA = E$. Kasutades neid võrdusi ja maatriksite korrutamise assotsiatiivsust saame, et

$$B = BE = B(AC) = (BA)C = EC = C.$$

□

Maatriksi A pöördmaatriksit tähistatakse sümboliga A^{-1}. Definitsioonist 3.1 näeme, et kui B on A pöördmaatriks, siis A on B pöördmaatriks. Seega võib öelda, et

$$\boxed{(A^{-1})^{-1} = A.}$$

Järgmine lause annab eeskirja maatriksite korrutise pöördmaatriksi leidmiseks, kui on teada tegurite pöördmaatriksid.

Lause 3.3 *Kui ruutmaatriksid $A, B \in \mathrm{Mat}_n$ on pööratavad, siis ka maatriks AB on pööratav, kusjuures*

$$\boxed{(AB)^{-1} = B^{-1}A^{-1}.}$$

Tõestus. Tõepoolest,

$$(AB)\left(B^{-1}A^{-1}\right) = A\left(B\left(B^{-1}A^{-1}\right)\right) = A\left(\left(BB^{-1}\right)A^{-1}\right) = A\left(EA^{-1}\right) = AA^{-1} = E$$

ja analoogiliselt $\left(B^{-1}A^{-1}\right)(AB) = E$. Definitsiooni 3.1 põhjal on $B^{-1}A^{-1}$ maatriksi AB pöördmaatriks. □

Definitsioon 3.4 Ruutmaatriksit A nimetatakse **regulaarseks**, kui $|A| \neq 0$.

Lause 3.5 *Iga pööratav ruutmaatriks on regulaarne.*

TÕESTUS. Olgu maatriks $A \in \mathrm{Mat}_n$ pööratav. Siis tal leidub pöördmaatriks A^{-1} nii, et $AA^{-1} = E$. Kuna teoreemi 2.33 põhjal on korrutise determinant võrdne tegurite determinantide korrutisega, siis $1 = |E| = |AA^{-1}| = |A| \cdot |A^{-1}|$. Järelikult $|A| \neq 0$. □

Defineerime nüüd elementaarteisendused maatriksi ridadega. Selliseid teisendusi kasutatakse paljude praktiliste ülesannete lahendamisel (pöördmaatriksi leidmine, maatriksi astaku leidmine, lineaarvõrrandisüsteemi lahendamine jne.).

Definitsioon 3.6 Elementaarteisendused maatriksi ridadega on järgmised teisendused:

1. maatriksi kahe rea äravahetamine;
2. maatriksi rea korrutamine nullist erineva arvuga;
3. maatriksi mingile reale mingi arvuga korrutatud teise rea liitmine.

Analoogiliselt defineeritakse elementaarteisendused maatriksi veergudega.

Lause 3.7 *Maatriksi ridade äravahetamise saab taandada teistsugust tüüpi elementaarteisendustele ridadega*

TÕESTUS. Olgu meil vaja vahetada ära maatriksi A i-s ja j-s rida. Toimime selleks järgmiselt. Liidame i-ndale reale j-nda rea. Siis liidame saadud maatriksis j-ndale reale (-1)-ga korrutatud i-nda rea. Seejärel liidame i-ndale reale j-nda rea. Sellega oleme teinud kolm 3. tüüpi elementaarteisendust. Lõpuks korrutame j-nda rea (-1)-ga ja saamegi tulemuseks nõutava maatriksi. □

Loomulikult kehtib analoogiline tulemus ka veergude kohta.

Näitame nüüd, et elementaarteisenduste sooritamiseks maatriksi ridade või veergudega võib seda maatriksit korrutada teatud erikujuliste maatriksitega, mis on küllaltki sarnased ühikmaatriksile.

Olgu n fikseeritud naturaalarv. Iga $c \in \mathbb{R} \setminus \{0\}$ ja $i \in \{1, 2, \ldots, n\}$ korral olgu $E_i(c)$ n-ndat järku ruutmaatriks, mille peadiagonaali i-s element on c, teised peadiagonaali elemendid on 1-d ja kõik ülejäänud elemendid on 0-d, s.t. $E_i(c)$ on maatriks kujul

$$E_i(c) = \begin{pmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & c & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & \ldots & 1 \end{pmatrix}.$$

Iga $c \in \mathbb{R}$ ja $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, korral olgu $E_{ij}(c)$ maatriks, mille peadiagonaalil on 1-d, i-nda rea ja j-nda veeru element on c ja kõik ülejäänud elemendid on 0-d. Seega juhul, kui

$i < j$, on maatriks $E_{ij}(c)$ kujul

$$E_{ij}(c) = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & \dots & c & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix}.$$

Definitsioon 3.8 Maatrikseid $E_i(c)$ ja $E_{ij}(c)$ nimetatakse **n-indat järku elementaarmaatriksiteks**.

Lause 3.9 *Elementaarteisenduste tegemine maatriksi ridadega (veergudega) on samaväärne maatriksi korrutamisega vasakult (paremalt) teatud arvu elementaarmaatriksitega.*

Tõestus. Vaatleme maatriksit $A \in \mathrm{Mat}_n$. Leides korrutise $E_i(c)A$ näeme, et see on maatriks, mis on saadud maatriksist A i-nda rea korrutamisel c-ga. Samuti on lihtne veenduda, et $E_{ij}(c)A$ on maatriks, mis on saadud maatriksist A i-ndale reale c-kordse j-nda rea liitmisel. Lause 3.7 põhjal taandub ridade vahetus teatud arvule 2. ja 3. tüüpi elementaarteisendustele, seega samuti elementaarmaatriksitega vasakult korrutamisele.

Tõestus veergude jaoks on analoogiline. □

Lause 3.10 *Kõik elementaarmaatriksid on pööratavad, kusjuures ka nende pöördmaatriksid on elementaarmaatriksid.*

Tõestus. Vahetu kontroll näitab, et

$$(E_i(c))^{-1} = E_i\left(\frac{1}{c}\right)$$

ja

$$(E_{ij}(c))^{-1} = E_{ij}(-c).$$

□

Lause 3.11 *Kui A on regulaarne maatriks ja maatriks B on saadud maatriksist A ridade või veergude elementaarteisenduste abil, siis ka B on regulaarne.*

Tõestus. Lausetest 2.23, 2.21 ja 2.25 järeldub, et kui $|A| \neq 0$, siis ühegi elementaarteisenduse tulemusena saadud maatriksi determinant ei ole 0. □

Lause 3.12 *Iga regulaarse maatriksi saab ridade elementaarteisenduste abil teisendada ühikmaatriksiks.*

Tõestus. Järelduse 2.19 tõttu peab regulaarse maatriksi esimeses veerus leiduma nullist erinev element. Ridade vahetamise abil võime saavutada olukorra, kus see element asub kohal $(1,1)$. Vaatleme nüüd regulaarset maatriksit $A = (a_{ij}) \in \mathrm{Mat}_n$, kus $a_{11} \neq 0$. Liidame maatriksi A i-ndale reale, kus $i \in \{2, \ldots, n\}$, arvuga $-\frac{a_{i1}}{a_{11}}$ korrutatud esimese rea. Korrutades veel esimese rea nullist erineva arvuga $\frac{1}{a_{11}}$ jõuame maatriksini B, mis on kujul

$$B = \begin{pmatrix} 1 & b_{12} & b_{13} & \ldots & b_{1n} \\ 0 & b_{22} & b_{23} & \ldots & b_{2n} \\ 0 & b_{32} & b_{33} & \ldots & b_{3n} \\ \ldots & \ldots & \ldots & \ldots & \\ 0 & b_{n2} & b_{n3} & \ldots & b_{nn} \end{pmatrix}.$$

Lause 3.11 põhjal on B regulaarne. Arendades B determinanti esimese veeru järgi näeme, et $|B| = |B'|$, kus

$$B' = \begin{pmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \ldots & \ldots & \ldots & \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{pmatrix}.$$

Seega ka B' on regulaarne maatriks ja tema esimeses veerus (s.t. elementide $b_{22}, b_{32}, \ldots, b_{n2}$ hulgas) peab leiduma nullist erinev element. Tõstes sarnasel moel nullist erinevaid elemente peadiagonaalile ja muutes neist allapoole jäävaid elemente nullideks jõuame ridade elementaarteisenduste abil maatriksini

$$C = \begin{pmatrix} 1 & c_{12} & c_{13} & \ldots & c_{1,n-1} & c_{1n} \\ 0 & 1 & c_{23} & \ldots & c_{2,n-1} & c_{2n} \\ 0 & 0 & 1 & \ldots & c_{3,n-1} & c_{3n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & c_{n-1,n} \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix},$$

s.t. ülemise kolmnurkmaatriksini, mille peadiagonaalil on 1-d. Liigume nüüd veerge vaadeldes paremalt vasakule. Liidame maatriksi C i-ndale reale, kus $i \in \{1, 2, \ldots, n-1\}$, arvuga $-c_{in}$ korrutatud n-nda rea. Sellega muutuvad nulliks kõik elemendid viimases veerus, välja arvatud viimane element. Samamoodi toimime eelviimase, üle-eelviimase jne. veeruga, kuni oleme jõudnud ühikmaatriksini. □

Järgmine tulemus ütleb, et maatriksi pööratavuse üle saab otsustada tema determinandi põhjal.

Teoreem 3.13 *Ruutmaatriks on pööratav parajasti siis, kui ta on regulaarne.*

Tõestus. Tarvilikkus. See on tõestatud lauses 3.5.
Piisavus. Olgu $A \in \mathrm{Mat}_n$ regulaarne maatriks. Nagu näitasime lauses 3.12, saab maatriksi A ridade elementaarteisenduste abil teisendada ühikmaatriksiks. Lause 3.9 põhjal on elementaarteisenduste tegemine maatriksi ridadega samaväärne maatriksi korrutamisega vasakult teatud arvu elementaarmaatriksitega. Seega leiduvad sellised elementaarmaatriksid $E_1, E_2, \ldots, E_k$, et

$$E_k \ldots E_2 E_1 A = E.$$

Tähistame $B := E_k \dots E_2 E_1$, siis $BA = E$. Et elementaarmaatriksid on pööratavad (lause 3.10), siis on ka B pööratav ja lauset 3.3 $k-1$ korda rakendades saame, et

$$B^{-1} = E_1^{-1} E_2^{-1} \dots E_k^{-1}.$$

Korrutame võrduse $BA = E$ mõlemad pooled vasakult maatriksiga B^{-1}. See annab meile võrduse $B^{-1}(BA) = B^{-1}E$, millest järeldub, et

$$A = EA = (B^{-1}B)A = B^{-1}(BA) = B^{-1}E = B^{-1}.$$

Järelikult $B = (B^{-1})^{-1} = A^{-1}$. □

Järeldus 3.14 *Iga regulaarse maatriksi saab esitada elementaarmaatriksite korrutisena.*

Tõestus. Teoreemi 3.13 tõestuses nägime, et kui A on regulaarne, siis $A = E_1^{-1} E_2^{-1} \dots E_k^{-1}$, kus maatriksid $E_1, \dots, E_k$ on elementaarmaatriksid. Tänu lausele 3.10 on ka $E_1^{-1}, \dots, E_k^{-1}$ elementaarmaatriksid. □

Märkus 3.15 Viimast fakti kasutatakse muuhulgas matemaatilises analüüsis kordsete integraalide muutujavahetuse juures.

Teoreemi 3.13 tõestuses nägime, et $A^{-1} = E_k \dots E_2 E_1 = E_k \dots E_2 E_1 E$. See tähendab, et maatriksi A pöördmaatriksi saamiseks tuleb ühikmaatriksi E ridadega teha täpselt samad teisendused (ja täpselt samas järjekorras), mis maatriksi A ridadegagi, et saada A-st ühikmaatriks. See annab meile järgmise praktilise meetodi A pöördmaatriksi leidmiseks. Koostame $(n \times 2n)$-indat järku maatriksi nii, et kirjutame A kõrvale paremale n-indat järku ühikmaatriksi:

$$(A|E).$$

Teeme selle maatriksi ridadega elementaarteisendusi eesmärgiga saada vasakule poole ühikmaatriks. Eelpoolöeldut arvestades jõuame lõpuks maatriksini

$$(E|A^{-1}),$$

mille põhjal saame välja kirjutada A pöördmaatriksi.

Pöördmaatriksi leidmiseks on ka veel teine võimalus, nimelt determinantide abil.

Teoreem 3.16 *Kui $A = (a_{ij}) \in \mathrm{Mat}_n$ on regulaarne, siis*

$$\boxed{A^{-1} = \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix},}$$

kus A_{ij} on maatriksi A elemendi a_{ij} algebraline täiend.

Tõestus. Tähistame

$$A^* := \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}.$$

Vastavalt maatriksite korrutamise eeskirjale on korrutise AA^* i-nda rea ja i-nda veeru ($i \in \{1, \ldots, n\}$) element

$$a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in} = \sum_{k=1}^{n} a_{ik}A_{ik} = |A|,$$

kus viimane võrdus kehtib Laplace'i teoreemi põhjal, sest tegemist on $|A|$ arendisega i-nda rea järgi (vt. võrdust (18)). Kui $i \neq j$, $i, j \in \{1, \ldots, n\}$, siis korrutise AA^* i-nda rea ja j-nda veeru element on

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn} = \sum_{k=1}^{n} a_{ik}A_{jk}.$$

Moodustame maatriksi B, mille kõik read, välja arvatud j-s rida on samad, mis maatriksil A, j-indaks reaks on aga maatriksi A i-s rida. Et maatriksis B on kaks võrdset rida, siis $|B| = 0$. Teisest küljest, arendades maatriksi B determinanti j-nda rea järgi saame võrduse $|B| = \sum_{k=1}^{n} a_{ik}A_{jk}$ (sest elemendi a_{ik} algebraline täiend maatriksis B on sama, mis elemendi a_{jk} algebraline täiend maatriksis A, s.t. A_{jk}). Seega $\sum_{k=1}^{n} a_{ik}A_{jk} = 0$, mis tähendab, et maatriksi AA^* kõik väljaspool peadiagonaali asuvad elemendid on 0-d. Sellega oleme näidanud, et

$$AA^* = \begin{pmatrix} |A| & 0 & \ldots & 0 \\ 0 & |A| & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & |A| \end{pmatrix} = |A| \cdot E.$$

Arutledes analoogiliselt veergudega saame võrduse $A^*A = |A| \cdot E$. Et A on regulaarne, siis $|A| \neq 0$ ja on olemas arv $\frac{1}{|A|}$. Korrutades selle arvuga võrduste $AA^* = |A| \cdot E$ ja $A^*A = |A| \cdot E$ mõlemaid pooli ja kasutades lauset 1.27(5) saame

$$A \cdot \left(\frac{1}{|A|} \cdot A^* \right) = E = \left(\frac{1}{|A|} \cdot A^* \right) \cdot A,$$

mis tänu pöördmaatriksi definitsioonile tähendabki, et

$$A^{-1} = \frac{1}{|A|} \cdot A^*.$$

□

Tõestatud teoreemist saab lihtsa vaevaga tuletada valemi teist järku ruutmaatriksi pöördmaatriksi leidmiseks.

Järeldus 3.17 *Kui $ad - bc \neq 0$, siis*

$$\boxed{\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.}$$

Näide 3.18 Leiame maatriksi

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 1 & 2 \\ 3 & 5 & 7 \end{pmatrix}$$

pöördmaatriksi. Arvutades maatriksi A determinandi ja kõigi elementide algebralised täiendid, saame

$$\begin{aligned}
|A| &= \begin{vmatrix} 2 & 3 & 4 \\ 1 & 1 & 2 \\ 3 & 5 & 7 \end{vmatrix} \overset{-2\mathrm{I}}{=} \begin{vmatrix} 2 & 3 & 0 \\ 1 & 1 & 0 \\ 3 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 3 \\ 1 & 1 \end{vmatrix} = -1, \\
A^{-1} &= \frac{1}{|A|}(A_{ij})^T = \frac{1}{-1} \begin{pmatrix} \begin{vmatrix} 1 & 2 \\ 5 & 7 \end{vmatrix} & -\begin{vmatrix} 3 & 4 \\ 5 & 7 \end{vmatrix} & \begin{vmatrix} 3 & 4 \\ 1 & 2 \end{vmatrix} \\ -\begin{vmatrix} 1 & 2 \\ 3 & 7 \end{vmatrix} & \begin{vmatrix} 2 & 4 \\ 3 & 7 \end{vmatrix} & -\begin{vmatrix} 2 & 4 \\ 1 & 2 \end{vmatrix} \\ \begin{vmatrix} 1 & 1 \\ 3 & 5 \end{vmatrix} & -\begin{vmatrix} 2 & 3 \\ 3 & 5 \end{vmatrix} & \begin{vmatrix} 2 & 3 \\ 1 & 1 \end{vmatrix} \end{pmatrix} \\
&= -\begin{pmatrix} -3 & -1 & 2 \\ -1 & 2 & 0 \\ 2 & -1 & -1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & -2 \\ 1 & -2 & 0 \\ -2 & 1 & 1 \end{pmatrix}.
\end{aligned}$$

Lõpuks näitame, kuidas on omavahel seotud pöördmaatriksi leidmine ja transponeerimine.

Lause 3.19 *Kui A on pööratav ruutmaatriks, siis*

$$\boxed{(A^T)^{-1} = \left(A^{-1}\right)^T.}$$

Tõestus. Kuna

$$\begin{aligned}
\left(A^{-1}\right)^T A^T &= \left(AA^{-1}\right)^T = E^T = E, \\
A^T \left(A^{-1}\right)^T &= \left(A^{-1}A\right)^T = E^T = E,
\end{aligned}$$

siis definitsiooni põhjal on $\left(A^{-1}\right)^T$ maatriksi A^T pöördmaatriks. □

4 Algebralised struktuurid

Algebraline struktuur on hulk, millel on defineeritud mingid tehted, mis rahuldavad teatud tingimusi. Käesolevas kursuses tutvume vaid kõige tähtsamate ja klassikalisemate algebraliste struktuuride definitsioonidega. Nendeks on rühm, ring, korpus ja vektorruum. Algebralisi struktuure uurib algebra haru, mida kutsutakse abstraktseks algebraks.

4.1 Rühm

Definitsioon 4.1 Kahekohaline (ehk **binaarne) algebraline tehe** hulgal A on kujutus hulgast $A \times A$ hulka A.

Märkus 4.2 Sõna "algebraline" eelmises definitsioonis rõhutab seda, et tehte tulemus kuulub ka hulka A. Põhimõtteliselt võib vaadelda ka kahekohalisi tehteid $A \times A \to B$, kus $B \neq A$. Näiteks kolmemõõtmelise ruumi vabavektorite liitmine on algebraline tehe $\mathbb{E}_3 \times \mathbb{E}_3 \to \mathbb{E}_3$, aga skalaarkorrutamine on tehe $\mathbb{E}_3 \times \mathbb{E}_3 \to \mathbb{R}$, mis ei ole algebraline.

Niisiis kahekohaline algebraline tehe hulgal A on eeskiri, mis igale hulga A elementide järjestatud paarile (a, b) seab vastavusse hulga A mingi elemendi. Kahekohalisest tehtest rääkides kirjutatakse tehtemärk harilikult hulga elementide vahele. Seega kahekohalise tehte $* : A \times A \to A$ korral kirjutatakse $*((a, b))$ asemel harilikult $a * b$ ja võib öelda, et tehe $*$ seab paarile (a, b) vastavusse hulga A elemendi $a * b$.

Näide 4.3 Naturaalarvude hulgal $\mathbb{N}$ võib vaadelda kahekohalisi algebralisi tehteid, mis on defineeritud näiteks järgmiste eeskirjadega:

- $(a, b) \mapsto a + b$;
- $(a, b) \mapsto a^b$;
- $(a, b) \mapsto b + 5$;
- $(a, b) \mapsto ab$;
- $(a, b) \mapsto b^a$;
- $(a, b) \mapsto 3$;

Lahutamistehe ei ole algebraline tehe hulgal $\mathbb{N}$, sest näiteks $1 - 2 \notin \mathbb{N}$.

Definitsioon 4.4 Rühm on hulk G koos kahekohalise algebralise tehtega $*$, mis rahuldab järgmisi tingimusi:

G1. $(a * b) * c = a * (b * c)$ iga $a, b, c \in G$ korral;

G2. leidub element $e \in G$ nii, et $a * e = a = e * a$ iga $a \in G$ korral;

G3. iga $a \in G$ korral leidub element $b \in G$ nii, et $a * b = e = b * a$.

Elementi e tingimuses G2 nimetatakse rühma G **ühikelemendiks** ja elementi b tingimuses G3 nimetatakse elemendi a **pöördelemendiks**.

Teiste sõnadega võib öelda, et rühm on hulk, millel on defineeritud kahekohaline assotsiatiivne tehe, mille suhtes leidub ühikelement ja mille suhtes leidub igal elemendil pöördelement.

Kui tahetakse ära näidata, milline on vaadeldava rühma tehe, siis kirjutatakse vahel rühma paarina $(G, *)$.

Rääkides rühmadest üldiselt kutsume tehet $*$ kokkuleppeliselt korrutamiseks ja elementi $a * b$ elementide a ja b korrutiseks.

Näide 4.5 1. Nullist erinevate ratsionaalarvude ja nullist erinevate reaalarvude hulgad on rühmad korrutamise suhtes. Seega võime vaadelda rühmi $(\mathbb{R} \setminus \{0\}, \cdot)$ ja $(\mathbb{Q} \setminus \{0\}, \cdot)$.

2. Positiivsete ratsionaalarvude ja positiivsete reaalarvude hulgad on rühmad korrutamise suhtes.

3. Hulgad $\mathbb{Z}, \mathbb{Q}$ ja $\mathbb{R}$ on rühmad liitmise suhtes.

4. Hulk $\{1, -1\}$ on rühm korrutamise suhtes.

5. Mittetühja hulga M bijektiivsete teisenduste hulk $S(M)$ on rühm kujutuste järjestrakendamise suhtes. Selle rühma ühikelement on hulga M samasusteisendus ja teisenduse f pöördelement on selle teisenduse pöördteisendus. Muuhulgas on ka substitutsioonide hulk S_n rühm. Seda rühma nimetatakse **sümmeetriliseks rühmaks** n-elemendilisel hulgal.

6. n-ndat järku regulaarsete maatriksite hulk on rühm maatriksite korrutamise suhtes. Selle rühma ühikelement on ühikmaatriks ja regulaarse maatriksi pöördelement selles rühmas on selle maatriksi pöördmaatriks. Sellist rühma tähistatakse harilikult $GL_n(\mathbb{R})$ (inglise keeles *general linear group*).

Lause 4.6 *Rühma ühikelement ja iga elemendi pöördelement on üheselt määratud.*

Tõestus. Olgu e ja f rühma $(G, *)$ ühikelemendid. Kuna e on ühikelement, siis $f = e * f$. Et f on ühikelement, siis $e * f = e$. Järelikult $f = e * f = e$.

Oletame nüüd, et elemendid b ja c on elemendi a pöördelemendid. Siis

$$c \underset{G2}{=} e * c \underset{G3}{=} (b * a) * c \underset{G1}{=} b * (a * c) \underset{G3}{=} b * e \underset{G2}{=} b.$$

Sellega oleme näidanud, et elemendi a pöördelement on üheselt määratud. □

Rühma ühikelementi tähistatakse tihti ka sümboliga 1. Elemendi a (üheselt määratud) pöördelementi tähistatakse sümboliga a^{-1}. Pöördelemendi definitsioonist on selge, et rühma G iga elemendi a korral

$$(a^{-1})^{-1} = a.$$

Lause 4.7 *Rühma $(G, *)$ mistahes elementide a ja b korral*

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

Tõestus. Tõepoolest,

$$(a * b) * (b^{-1} * a^{-1}) \underset{G1}{=} ((a * b) * b^{-1}) * a^{-1} \underset{G1}{=} (a * (b * b^{-1})) * a^{-1} \underset{G3}{=} (a * e) * a^{-1} \underset{G2}{=} a * a^{-1} \underset{G3}{=} e,$$

ning analoogiliselt saab tõestada võrduse $(b^{-1} * a^{-1}) * (a * b) = e$. □

Kui meil on kahekohaline algebraline tehe $*$ hulgal A ja rohkem kui kaks hulga A elementi, siis sulgude abil saab ära näidata, millises järjekorras me tehet $*$ neile elementidele peame rakendama. Näiteks kirjapanek $a * (b * c)$ näitab, et kõigepäält tuleb leida element $b * c$ ning seejärel rakendada tehet $*$ elementidele a ja $b * c$. Tulemuseks on hulga A mingi element. Kolme elemendi korral on kaks võimalust sulgude paigutamiseks: $(a * b) * c$ ja $a * (b * c)$. Kui elemente on rohkem, siis on ka sulgude paigutamise võimalusi rohkem, näiteks $(a * b) * (c * d)$, $((a * b) * c) * d$, $a * ((b * c) * d)$ jne. Osutub, et assotsiatiivse tehte korral ei sõltu tehete tulemuseks saadav element sulgude paigutusest.

Lause 4.8 *Kui $*$ on assotsiatiivne kahekohaline algebraline tehe hulgal A, siis tulemus, mille saame tehte rakendamisel hulga A elementidele, ei sõltu sulgude paigutusest.*

TÕESTUS. Olgu $*$ assotsiatiivne kahekohaline algebraline tehe hulgal A. Tõestame matemaatilise induktsiooniga, et iga $n \in \mathbb{N}$ ja mistahes elementide $a_1, \ldots, a_n \in A$ korral ei sõltu tehte $*$ neile elementidele rakendamise tulemus sulgude paigutusest.

Kui $n = 1$ või $n = 2$, siis on väide ilmne. Kui $n = 3$, siis järeldub väide tehte $*$ assotsiatiivsusest. Olgu nüüd $n > 3$ ja eeldame, et väide kehtib, kui elemente on vähem kui n. Tähistame iga $k \in \mathbb{N}$ ja $b_1, \ldots, b_k \in A$ korral

$$b_1 * b_2 * \ldots * b_k := (\ldots((b_1 * b_2) * b_3) * \ldots * b_{k-1}) * b_k. \tag{20}$$

Induktsiooni eelduse põhjal on mistahes sulgude paigutusega avaldis vähem kui n elemendist võrdne sellisel kujul avaldisega. Tõestuse lõpetamiseks piisab näidata, et sama omadus on ka igal n elemendist moodustatud avaldisel. Vaatleme sellist avaldist ja leiame selles üles tehte $*$ viimase rakendamise:

$$(a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_n). \tag{21}$$

Siin sulgudes olevad avaldised võib kirjutada kujul (20), sest neis esineb vähem kui n elementi. On kaks võimalust.

1) $k = n - 1$. Siis on avaldis (21) kujul $(a_1 * \ldots * a_{n-1}) * a_n = a_1 * \ldots * a_{n-1} * a_n$, s.t. kujul (20).

2) $k < n - 1$. Siis kasutades assotsiatiivsuse omadust ja induktsiooni eeldust elementide $a_1, \ldots, a_{n-1}$ korral võime kirjutada

$$\begin{aligned}
(a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_n) &= (a_1 * \ldots * a_k) * ((a_{k+1} * \ldots * a_{n-1}) * a_n) \\
&= ((a_1 * \ldots * a_k) * (a_{k+1} * \ldots * a_{n-1})) * a_n \\
&= (a_1 * \ldots * a_k * a_{k+1} * \ldots * a_{n-1}) * a_n \\
&= a_1 * \ldots * a_k * a_{k+1} * \ldots * a_{n-1} * a_n,
\end{aligned}$$

s.t. jällegi on avaldis võrdne avaldisega kujul (20). □

Arvestades lauset 4.8 jäetakse assotsiatiivse tehte korral sulud tihti üldse kirjutamata.

Definitsioon 4.9 Rühma $(G, *)$ nimetatakse **kommutatiivseks** ehk **Abeli rühmaks**, kui iga $a, b \in G$ korral

$$a * b = b * a.$$

Näide 4.10 Näite 4.5 neljas esimeses punktis loetletud rühmad on kommutatiivsed. Rühm S_3 ei ole kommutatiivne.

Abeli rühmadest üldiselt kõneldes on tavaks kasutada nn. aditiivset sümboolikat. Tehtemärgina kasutatakse märki + ja tehet kutsutakse liitmiseks, ühikelementi kutsutakse nullelemendiks ja kasutatakse sümbolit 0, elemendi a pöördelementi kutsutakse vastandelemendiks ja tähistatakse sümboliga $-a$. Seega Abeli rühma definitsiooni võib sõnastada järgmisel kujul.

Definitsioon 4.11 Abeli rühm on hulk A koos kahekohalise algebralise tehtega $+$, mis rahuldab järgmisi tingimusi:

AG1. $(a + b) + c = a + (b + c)$ iga $a, b, c \in A$ korral;

AG2. leidub element $0 \in A$ nii, et $a + 0 = a = 0 + a$ iga $a \in A$ korral;

AG3. iga $a \in A$ korral leidub element $-a \in A$ nii, et $a + (-a) = 0 = (-a) + a$;

AG4. $a + b = b + a$ iga $a, b \in A$ korral.

Abeli rühma korral räägitakse ka elementide a ja b **vahest**, mis defineeritakse võrdusega

$$a - b := a + (-b).$$

Tingimuse AG3 põhjal on selge, et iga a korral

$$a - a = 0.$$

4.2 Ring ja korpus

Vaatleme nüüd kahe kahekohalise algebralise tehtega struktuure.

Definitsioon 4.12 Ring on hulk R koos kahe kahekohalise algebralise tehtega $+$ ja $\cdot$, mis rahuldavad järgmisi tingimusi:

R1. $(a + b) + c = a + (b + c)$ iga $a, b, c \in R$ korral;

R2. leidub element $0 \in R$ nii, et $a + 0 = a = 0 + a$ iga $a \in R$ korral;

R3. iga $a \in R$ korral leidub element $-a \in R$ nii, et $a + (-a) = 0 = (-a) + a$;

R4. $a + b = b + a$ iga $a, b \in R$ korral;

R5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ iga $a, b, c \in R$ korral;

R6. leidub element $1 \in R$ nii, et $a \cdot 1 = a = 1 \cdot a$ iga $a \in R$ korral;

R7. $a \cdot (b + c) = a \cdot b + a \cdot c$ iga $a, b, c \in R$ korral;

R8. $(a + b) \cdot c = a \cdot c + b \cdot c$ iga $a, b, c \in R$ korral.

Harilikult kirjutatakse ringi puhul $a \cdot b$ asemel lühemalt ab. Definitsiooni tingimustest R1–R4 näeme, et ring peab liitmise suhtes olema Abeli rühm. Tingimusi R7 ja R8 kutsutakse **distributiivsuse seadusteks**.

Definitsioon 4.13 Ringi nimetatakse **kommutatiivseks**, kui tema korrutamistehe on kommutatiivne.

Definitsioon 4.14 Korpus on kommutatiivne ring, milles on vähemalt kaks elementi ja mille igal nullelemendist erineval elemendil leidub pöördelement korrutamise suhtes.

Arvestades tingimusi R5 ja R6 näeme, et korpuse nullelemendist erinevad elemendid moodustavad rühma korrutamise suhtes.

Märkus 4.15 Eestikeelses kirjanduses (nt. [1], [2]) ei ole tihti nõutud, et korpuse korrutamine oleks kommutatiivne. Käesolevas kursuses me seda siiski nõuame ja loodame, et sellest ei teki segadust.

Näide 4.16 1. $(\mathbb{Z}, +, \cdot)$ on kommutatiivne ring, mis ei ole korpus (nt. elemendil $2 \in \mathbb{Z}$ ei leidu pöördelementi ringis $\mathbb{Z}$).

2. $(\mathbb{Q}, +, \cdot)$ ja $(\mathbb{R}, +, \cdot)$ on korpused.

3. Hulk Mat_n on ring maatriksite liitmise ja korrutamise suhtes. See on tõestatud lause 1.24 punktides 1–4 ja lause 1.27 punktides 1–4. Ruutmaatriksite ringi nullelement on nullmaatriks ja ühikelement on ühikmaatriks. Kui $n \geqslant 2$, siis see ring ei ole kommutatiivne. Selles ringis on näiteks nullmaatriksist erinev maatriks

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

mittepööratav.

Lause 4.17 *Mistahes ringis R kehtivad järgmised arvutusreeglid:*

1. *iga $a, b, c \in R$ korral kui $a + b = c$, siis $a = c - b$;*
2. *$0a = 0 = a0$ iga $a \in R$ korral;*
3. *$(-a)b = a(-b) = -(ab)$ iga $a, b \in R$ korral;*
4. *$a(b - c) = ab - ac$ iga $a, b, c \in R$ korral;*
5. *$(a - b)c = ac - bc$ iga $a, b, c \in R$ korral.*

Tõestus. 1. Kehtigu võrdus $a + b = c$, kus $a, b, c \in R$. Liites selle võrduse mõlemale poolele elemendi $-b$ saame

$$(a + b) + (-b) = c + (-b) = c - b.$$

Kuna

$$(a + b) + (-b) \underset{R1}{=} a + (b + (-b)) \underset{R3}{=} a + 0 \underset{R2}{=} a,$$

siis saamegi võrduse $a = c - b$.

2. Olgu $a \in R$. Siis

$$0a \underset{R2}{=} (0 + 0)a \underset{R8}{=} 0a + 0a.$$

Kasutades eespool tõestatud omadust 1 saame võrduse

$$0a = 0a - 0a \underset{R3}{=} 0.$$

Võrduse $a0 = 0$ saab tõestada analoogiliselt.

3. Olgu $a, b \in R$. Siis

$$0 = 0b \underset{R3}{=} ((-a) + a)b \underset{R8}{=} (-a)b + ab.$$

Omaduse 1 põhjal

$$(-a)b = 0 - ab \underset{R2}{=} -ab.$$

Võrduse $a(-b) = -ab$ saab tõestada analoogiliselt.

4. Olgu $a, b, c \in R$. Siis

$$a(b - c) = a(b + (-c)) \underset{R7}{=} ab + a(-c) \underset{om.\ 3}{=} ab + (-ac) = ab - ac.$$

5. Võrduse $(a - b)c = ac - bc$ saab tõestada analoogiliselt. □

Märkus 4.18 Ringi puhul on võimalik, et $1 = 0$. Sellisel juhul see ring koosnebki ainult ühest elemendist, sest mistahes elemendi a korral $a = a1 = a0 = 0$. Järelikult, kui ringis on vähemalt kaks elementi, siis selles ringis $1 \neq 0$. Muuhulgas korpuses on alati $1 \neq 0$.

Märkus 4.19 Korpuste puhul (nt. $\mathbb{Q}$ ja $\mathbb{R}$ korral) räägitakse sageli jagamisest. Nimelt öeldakse, et korpuse K elemendi a ja nullist erineva elemendi b jagatis on element ab^{-1} ja tähistatakse seda elementi sümboliga $\frac{a}{b}$.

4.3 Jäägiklassiringid

Selles paragrahvis tutvume teatud lõplike ringidega, mida kasutatakse palju nii arvuteoorias kui arvutiteaduses.

Fikseerime mingi naturaalarvu $n \geqslant 2$. On teada, et iga täisarvu a jaoks leiduvad üheselt määratud täisarvud q, r nii, et

$$a = qn + r \quad \text{ja} \quad 0 \leqslant r < n.$$

Arvu r nimetatakse **jäägiks**, mis tekib arvu a jagamisel arvuga n ning arvude q ja r leidmist kutsutakse **jäägiga jagamiseks.**

Definitsioon 4.20 Öeldakse, et täisarv b **jagab** täisarvu a (ja kirjutatakse $b \mid a$), kui leidub selline täisarv c, et $bc = a$.

Teiste sõnadega võib öelda, et arv b jagab arvu a, kui a jagamisel arvuga b tekib jääk 0.
Lihtne on veenduda, et kui $a, b, c, d \in \mathbb{Z}$, $a \mid b$ ja $a \mid c$, siis $a \mid b \pm c$ ja $a \mid bd$.

Definitsioon 4.21 Öeldakse, et täisarvud a ja b on **kongruentsed** mooduli n järgi, kui $n \mid a-b$. Tähistus: $a \equiv b \pmod{n}$.

Lause 4.22 *Täisarvud a ja b on kongruentsed mooduli n järgi parajasti siis, kui nad annavad arvuga n jagades sama jäägi.*

Tõestus. Tarvilikkus. Olgu $a = qn + r$, kus $0 \leqslant r < n$. Eeldame, et $a \equiv b \pmod{n}$. Siis $n \mid a - b$, mis tähendab, et $nk = a - b$ mingi $k \in \mathbb{Z}$ korral. Järelikult

$$b = a - nk = qn + r - nk = (q - k)n + r.$$

Siit näeme, et ka b annab arvuga n jagamisel jäägi r.
Piisavus. Eeldame, et $a = q_1 n + r$ ja $b = q_2 n + r$, kus $q_1, q_2, r \in \mathbb{Z}$ ja $0 \leqslant r < n$. Siis $a - b = (q_1 - q_2)n$, mis tähendab, et $n \mid a - b$. □

Kuna seos "a ja b annavad arvuga n jagades sama jäägi" on ilmselt ekvivalentsiseos täisarvude hulgal, siis on ka kongruentsusseos (mooduli n järgi) ekvivalentsiseos täisarvude hulgal. Iga ekvivalentsiseose puhul võib vaadelda ekvivalentsiklasse selle seose järgi. Kongruentsusseose puhul tähistatakse arvu $a \in \mathbb{Z}$ ekvivalentsiklassi sümboliga $\overline{a}$ ja nimetatakse arvu a **jäägiklassiks** mooduli n järgi. Niisiis

$$\overline{a} \;=\; \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{b \in \mathbb{Z} \mid a \text{ ja } b \text{ annavad } n\text{-ga jagamisel sama jäägi}\}.$$

Nagu hulgateooriast teada, võib ekvivalentsiklassi esindajaks valida mistahes elemendi sellest ekvivalentsiklassist. Näiteks kui $n = 5$, siis $\overline{2} = \overline{17} = \overline{-8}$.

Et erinevaid jääke, mis n-ga jagamisel saab tekkida, on täpselt n tükki (need jäägid on $0, 1, \ldots, n-1$), siis mooduli n järgi on täpselt n jäägiklassi. Nende jäägiklasside hulka tähistatakse

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Defineerime nüüd tehted jäägiklasside hulgal.

Definitsioon 4.23 Jäägiklasside $\overline{a}, \overline{b} \in \mathbb{Z}_n$ **summa** ja **korrutis** defineeritakse võrdustega

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b}, \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b}. \end{aligned}$$

Lause 4.24 *Jäägiklasside liitmine ja korrutamine on korrektselt defineeritud.*

TÕESTUS. Korrektsuse tõestamiseks peame näitama, et tehte tulemus ei sõltu sellest, millised täisarvud me jäägiklasside esindajateks valime. Oletame, et $\overline{a_1} = \overline{a_2}$ ja $\overline{b_1} = \overline{b_2}$. Siis $n \mid a_1 - a_2$ ja $n \mid b_1 - b_2$. Järelikult $n \mid (a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$, s.t. $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ ja $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Et $a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2)$ ja n jagab selle võrduse paremat poolt, siis $n \mid a_1 b_1 - a_2 b_2$ ning järelikult $a_1 b_1 \equiv a_2 b_2 \pmod{n}$ ehk $\overline{a_1 b_1} = \overline{a_2 b_2}$. □

Teoreem 4.25 *Hulk $\mathbb{Z}_n$ on defineeritud tehete suhtes kommutatiivne ring. See ring on korpus parajasti siis, kui n on algarv.*

TÕESTUS. Tehete definitsioonidest ja täisarvude omadustest järeldub kergesti, et $\mathbb{Z}_n$ on kommutatiivne ring.

Tõestame teise väite. Oletame, et $\mathbb{Z}_n$ on korpus, kuid n ei ole algarv, s.t. leiduvad sellised $a, b \in \mathbb{N}$, $1 < a, b < n$, et $n = ab$. Siis $\overline{a}\overline{b} = \overline{n} = \overline{0}$, kuid $\overline{a} \neq \overline{0}$ ja $\overline{b} \neq \overline{0}$. Korpuse igal nullist erineval elemendil on olemas pöördelement. Korrutades võrduse $\overline{a}\overline{b} = \overline{0}$ mõlemad pooled elemendiga $\overline{a}^{-1}$ saame võrduse $\overline{b} = \overline{0}$, mis on vastuolus eelnevaga. Seega n peab olema algarv.

Oletame nüüd, et n on algarv. Võtame nullist erineva elemendi $\overline{a}$, kus $1 \leqslant a \leqslant n-1$, ringis $\mathbb{Z}_n$. Siis $\text{SÜT}(a, n) = 1$. On teada (lause 9.22 analoog täisarvude jaoks, vt. ka [1], lause 6.3.5), et sellisel juhul leiduvad $x, y \in \mathbb{Z}$ nii, et $ax + ny = 1$. Järelikult

$$\overline{1} = \overline{ax + ny} = \overline{ax} + \overline{ny} = \overline{a}\,\overline{x} + \overline{0}\,\overline{y} = \overline{a}\,\overline{x},$$

mis tähendab, et element $\overline{a}$ on pööratav Kuna iga nullist erinev element on pööratav, siis $\mathbb{Z}_n$ on korpus. □

Definitsioon 4.26 Ringe $\mathbb{Z}_n$, kus $n \in \mathbb{N}$, kutsutakse **jäägiklassiringideks**. Korpusi $\mathbb{Z}_p$, kus p on algarv, kutsutakse **jäägiklassikorpusteks**.

Näide 4.27 Kuna 5 on algarv, siis $\mathbb{Z}_5$ on korpus. Selles korpuses $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$ ja $\overline{4}^{-1} = \overline{4}$, sest $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{2} \cdot \overline{3} = \overline{1}$ ja $\overline{4} \cdot \overline{4} = \overline{1}$.

Ring $\mathbb{Z}_6$ ei ole korpus, sest näiteks nullist erineval elemendil $\overline{2}$ ei leidu pöördelementi.

4.4 Lineaaralgebra üle korpuste

Siiani oleme vaadelnud lineaaralgebra mõisteid (maatriks, determinant, pöördmaatriks) vaid üle reaalarvude. Tegelikult saab need mõisted defineerida ka siis, kui reaalarvude korpus asendada suvalise korpusega. Ka sel juhul saab tõestada kõik eespool vaadeldud tulemused (ühe erandiga) täpselt samamoodi nagu oleme seda teinud. Ainuke erinevus on see, et kohtades, kus oleme kasutanud reaalarvude jagatisi $\frac{a}{b}$ (näiteks teoreemis 3.16), tuleks nüüd kasutada korpuse elemente ab^{-1}. Lause 2.24 tõestust saab kasutada juhul kui korpuses $1+1 \neq 0$. See lause kehtib siiski ka maatriksite jaoks üle suvalise korpuse, sest seda saab tõestada lähtudes vahetult determinandi definitsioonist.

Kui K on korpus, siis sümboliga $\mathrm{Mat}_n(K)$ tähistatakse n-ndat järku ruutmaatriksite hulka, mille elemendid on korpusest K.

Näiteks maatriks

$$A = \begin{pmatrix} \overline{3} & \overline{2} \\ \overline{3} & \overline{4} \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}_5)$$

on pööratav, sest

$$|A| = \begin{vmatrix} \overline{3} & \overline{2} \\ \overline{3} & \overline{4} \end{vmatrix} = \overline{3} \cdot \overline{4} - \overline{3} \cdot \overline{2} = \overline{12} - \overline{6} = \overline{2} - \overline{1} = \overline{1} \neq 0.$$

5 Kompleksarvud

5.1 Kompleksarvude korpus

Meile hästituntud ratsionaalarvude hulk $\mathbb{Q}$ ja reaalarvude hulk $\mathbb{R}$ on korpused. Samuti nägime, et iga algarvu p jaoks on olemas p-elemendiline jäägiklassikorpus $\mathbb{Z}_p$. Kuigi reaalarvude korpusel on palju häid omadusi, on tal ka üks oluline puudus: temas ei ole võimalik leida võrrandi

$$x^2 = -1$$

lahendit (ja, nagu me teame, ka mitmete teiste ruutvõrrandite lahendeid). Sellest puudusest üle saamiseks konstrueeritakse üks suurem arvuhulk, mis sisaldab reaalarvude hulka ja kus antud võrrand on lahenduv. Seda suuremat hulka hakkame kutsuma kompleksarvude hulgaks. Kompleksarvude defineerimiseks on mitmeid võimalusi. Meie teeme seda defineerides järjestatud reaalarvupaaride hulgal $\mathbb{R}^2$ tehted sobival viisil.

Lause 5.1 *Hulk* $\mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$ *on korpus liitmise ja korrutamise suhtes, mis on defineeritud võrdustega*

$$\begin{aligned}(a,b)+(c,d) &= (a+c,b+d),\\ (a,b)(c,d) &= (ac-bd,bc+ad).\end{aligned}$$

Tõestus. Kuna $a+c, b+d, ac-bd, bc+ad \in \mathbb{R}$, siis on defineeritud liitmine ja korrutamine algebralised tehted hulgal $\mathbb{R}^2$. Lihtne on veenduda, et $(\mathbb{R}^2,+)$ on Abeli rühm, kus nullelemendiks on paar $(0,0)$ ja paari (a,b) vastandelement on paar $(-a,-b)$. Kui $a,b,c,d,e,f \in \mathbb{R}$, siis

$$\begin{aligned}((a,b)(c,d))(e,f) &= (ac-bd,bc+ad)(e,f)\\ &= ((ac-bd)e-(bc+ad)f,(bc+ad)e+(ac-bd)f)\\ &= (ace-bde-bcf-adf,bce+ade+acf-bdf)\\ &= (a(ce-df)-b(de+cf),b(ce-df)+a(de+cf))\\ &= (a,b)(ce-df,de+cf)\\ &= (a,b)((c,d)(e,f)),\\ (a,b)(c,d) &= (ac-bd,bc+ad) = (ca-db,da+cb) = (c,d)(a,b),\end{aligned}$$

mis tähendab, et korrutamine on assotsiatiivne ja kommutatiivne. Et mistahes $a,b \in \mathbb{R}$ korral

$$(a,b)(1,0) = (a\cdot 1 - b\cdot 0, b\cdot 1 + a\cdot 0) = (a,b)$$

ja kommutatiivsuse tõttu ka $(1,0)(a,b) = (a,b)$, siis $(1,0)$ on ühikelement korrutamise suhtes. Kui $a,b,c,d,e,f \in \mathbb{R}$, siis

$$\begin{aligned}(a,b)((c,d)+(e,f)) &= (a,b)(c+e,d+f)\\ &= (a(c+e)-b(d+f),b(c+e)+a(d+f))\\ &= (ac+ae-bd-bf,bc+be+ad+af)\\ &= (ac-bd,bc+ad)+(ae-bf,be+af)\\ &= (a,b)(c,d)+(a,b)(e,f)\end{aligned}$$

ja seega kehtib esimene distributiivsuse seadus. Teise kehtimine järeldub jällegi korrutamise kommutatiivsusest. Sellega oleme näidanud, et hulk $\mathbb{R}^2$ on defineeritud tehete suhtes ring.

Olgu nüüd $(a,b) \in \mathbb{R}^2$ nullelemendist $(0,0)$ erinev element, s.t. $a \neq 0$ või $b \neq 0$, millest järeldub, et $a^2+b^2 \neq 0$. Kuna

$$(a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{ba-ab}{a^2+b^2} \right) = (1,0),$$

siis

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \right) \in \mathbb{R}^2.$$

Sellega oleme näidanud, et $\mathbb{R}^2$ on defineeritud tehete suhtes korpus. □

Lauses 5.1 konstrueeritud korpust tähistame sümboliga $\mathbb{C}$ ja nimetame **kompleksarvude korpuseks.** Selle korpuse elemente kutsutakse **kompleksarvudeks**.

Lause 5.2 *Hulga $\mathbb{R}^2$ alamhulk $\mathbb{R}' = \{(a,0) \mid a \in \mathbb{R}\}$ on korpus lauses 5.1 defineeritud tehete suhtes.*

Tõestus. Kuna $(a,0)+(b,0) = (a+b,0)$ ja $(a,0)(b,0) = (ab-0, 0+0) = (ab,0)$ mistahes $a,b \in \mathbb{R}$ korral, siis defineeritud liitmine ja korrutamine on algebralised tehted hulgal $\mathbb{R}'$. Need tehted on ilmselt ka assotsiatiivsed, kommutatiivsed ja seotud distributiivsuse seadustega. Elemendid $(0,0)$ ja $(1,0)$ kuuluvad hulka $\mathbb{R}'$, seega on hulgas $\mathbb{R}'$ olemas ka nullelement ja ühikelement. Kui $(a,0) \in \mathbb{R}'$, siis on sellel elemendil olemas vastandelement $(-a,0) \in \mathbb{R}'$. Kui $(a,0) \in \mathbb{R}'$ ei ole nullelement (s.t. $a \neq 0$), siis on sellel elemendil hulgas $\mathbb{R}'$ olemas pöördelement $\left(\frac{1}{a}, 0\right)$. Kokkuvõttes oleme veendunud, et $\mathbb{R}'$ on korpus. □

Kui kahe sama tüüpi algebralise struktuuri vahel leidub üksühene vastavus (bijektsioon), mis säilitab tehted, siis neid struktuure nimetatakse isomorfseteks. Täpsemalt öeldes on sellel definitsioonil ringide korral järgmine kuju.

Definitsioon 5.3 Ringe R ja R' nimetatakse **isomorfseteks**, kui leidub bijektiivne kujutus $f : R \to R'$ nii, et

RH1. $f(a+b) = f(a) + f(b)$ mistahes $a,b \in R$ korral (s.t. f säilitab liitmise);

RH2. $f(ab) = f(a)f(b)$ mistahes $a,b \in R$ korral (s.t. f säilitab korrutamise);

RH3. $f(1) = 1$ (s.t. f säilitab ühikelemendi).

Sellist kujutust f nimetatakse **isomorfismiks** ringist R ringi R'. Kahte korpust nimetatakse **isomorfseteks**, kui nad on isomorfsed kui ringid.

Lause 5.4 *Reaalarvude korpus $\mathbb{R}$ on isomorfne korpusega $\mathbb{R}'$ lausest 5.2.*

Tõestus. Kujutus $f : \mathbb{R} \to \mathbb{R}', a \mapsto (a,0)$ on ilmselt bijektiivne. Kuna mistahes $a,b \in \mathbb{R}$ korral

$$\begin{aligned} f(a+b) &= (a+b,0) = (a,0)+(b,0) = f(a)+f(b), \\ f(ab) &= (ab,0) = (a \cdot b - 0 \cdot 0, 0 \cdot b + a \cdot 0) = (a,0)(b,0) = f(a)f(b), \\ f(1) &= (1,0), \end{aligned}$$

siis f on isomorfism. □

Arvestades isomorfismi korpuste $\mathbb{R}$ ja $\mathbb{R}'$ vahel samastatakse enamasti reaalarv a korpuse $\mathbb{C}$ elemendiga $(a,0)$. Seda samastamist arvestades võime korpuse $\mathbb{C}$ mistahes elemendi (a,b) kirjutada üles kujul

$$(a,b) = (a,0) + (0,b) = (a,0) + (b,0)(0,1) = a + bi,$$

kus oleme tähistanud $i := (0,1)$. Paneme tähele, et elemendi $i \in \mathbb{C}$ ruut on -1:

$$i^2 = (0,1)(0,1) = (0 \cdot 0 - 1 \cdot 1, 1 \cdot 0 + 0 \cdot 1) = (-1,0) = -1.$$

Seega võrrandil $x^2 = -1$ on korpuses $\mathbb{C}$ olemas lahend. Kompleksarvu i nimetatakse **imaginaarühikuks**.

Harilikult esitataksegi kompleksarve kujul

$$a + bi,$$

kus $a, b \in \mathbb{R}$. Sellist kuju nimetatakse kompleksarvu **algebraliseks kujuks**.

Kui b on negatiivne, siis harilikult kirjutatakse $a+bi$ asemel $a-|b|i$. Näiteks $2+(-3)i$ asemel kirjutatakse harilikult $2-3i$.

Definitsioon 5.5 Kui $z = a + bi$ on algebralisel kujul esitatud kompleksarv, siis

- reaalarvu a nimetatakse z **reaalosaks** (tähistatakse $a = \operatorname{Re} z$);
- kompleksarvu bi nimetatakse z **imaginaarosaks**;
- reaalarvu b nimetatakse z **imaginaarosa kordajaks** (tähistatakse $b = \operatorname{Im} z$).

Definitsioon 5.6 Kompleksarvu, mis ei ole reaalarv, nimetatakse **imaginaararvuks**. Imaginaararvu, mille reaalosa on 0, nimetatakse **puhtimaginaararvuks**.

Seega näiteks $5 + 2i$ on imaginaararv ja $-3i$ on puhtimaginaararv.

Kaks algebralisel kujul esitatud kompleksarvu $a + bi$ ja $c + di$ on võrdsed, kui järjestatud paarid (a, b) ja (c, d) on võrdsed. Seega

$$a + bi = c + di \iff a = c \text{ ja } b = d.$$

Teiste sõnadega: kaks kompleksarvu on võrdsed parajasti siis, kui nende kompleksarvude reaalosad on võrdsed ja imaginaarosa kordajad on võrdsed.

Algebralisel kujul näevad tehete definitsioonid välja järgmised:

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i, \\ (a + bi)(c + di) &= (ac - bd) + (bc + ad)i. \end{aligned}$$

Samuti kehtivad eelpoolöeldut arvestades võrdused

$$\begin{aligned} -(a + bi) &= -a - bi, \\ (a + bi)^{-1} &= \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i = \frac{1}{a^2 + b^2} \cdot (a - bi). \end{aligned}$$

Ka kompleksarvude korpuses võib rääkida nullist erineva arvuga jagamisest pidades selle all silmas pöördelemendiga korrutamist (vt. märkust 4.19). Seega

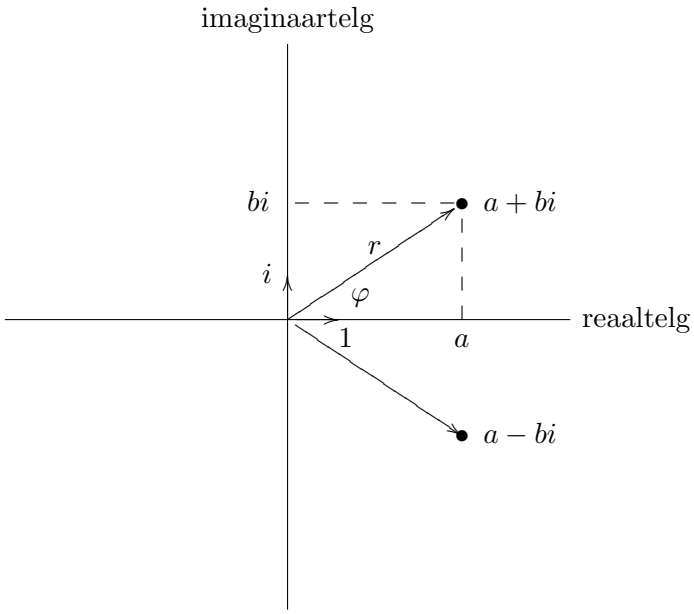
$$\frac{c + di}{a + bi} = (c + di) \cdot (a + bi)^{-1} = \frac{(c + di)(a - bi)}{a^2 + b^2}.$$

Selle eeskirja võib sõnastada järgmiselt: *selleks, et jagada kompleksarv $c + di$ nullist erineva kompleksarvuga $a + bi$ tuleb arv $c + di$ korrutada kompleksarvuga $a - bi$ ja tulemus reaalarvuga $\frac{1}{a^2+b^2}$.*

5.2 Kompleksarvude geomeetriline tõlgendus

Olgu antud tasand koos ristkoordinaadistikuga. Siis tekib üksühene vastavus selle tasandi punktide ja reaalarvupaaride (a, b) (nende punktide koordinaatide) vahel. Seega on ka kompleksarvud üksüheses vastavuses selle tasandi punktidega: kompleksarvule $a + bi$ vastab punkt koordinaatidega (a, b). Tasandit koos kirjeldatud vastavusega nimetatakse **komplekstasandiks**. Koordinaadistiku x-telge nimetatakse **reaalteljeks** ja y-telge **imaginaarteljeks**. Reaalteljel asuvad parajasti reaalarvudele vastavad punktid ning imaginaarteljel puhtimaginaararvudele ja 0-le vastavad punktid.

Võib vaadelda ka selle tasandi vabavektorite hulka. Iga punkti koordinaadid on selle punkti kohavektori koordinaadid. Teades, et vektorite liitmisel tuleb liita nende vastavad koordinaadid, võime öelda ka, et kompleksarvude liitmisele vastab nendele arvudele vastavate punktide kohavektorite liitmine.



Definitsioon 5.7 Kompleksarvu $z = a + bi$ **kaaskompleksarvuks** nimetatakse kompleksarvu $\overline{z} = a - bi$.

Seega antud kompleksarvule ja tema kaaskompleksarvule vastavad punktid komplekstasandil asetsevad sümmeetriliselt reaaltelje suhtes.

Definitsiooni põhjal on kohe selge, et iga kompleksarvu z korral $\overline{\overline{z}} = z$ ja et $\overline{z} = z$ parajasti siis, kui z on reaalarv (s.t. vastav punkt asub reaalteljel).

Osutub, et kaaskompleksarvu leidmine on kooskõlas kompleksarvude liitmise ja korrutamisega. Tõepoolest, kui $z = a + bi$ ja $w = c + di$, siis

$$\begin{aligned} \overline{z + w} &= \overline{(a + c) + (b + d)i} = (a + c) - (b + d)i = (a - bi) + (c - di) = \overline{z} + \overline{w}, \\ \overline{z \cdot w} &= \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = (a - bi) \cdot (c - di) = \overline{z} \cdot \overline{w}. \end{aligned}$$

Olgu nüüd komplekstasandil antud veel polaarkoordinaadistik, mis koosneb ühest fikseeritud punktist (poolusest) ja sellest punktist algavast kiirest (polaarteljest). Olgu poolus ja polaartelg valitud nii, et pooluseks on reaal- ja imaginaartelje lõikepunkt ja et polaartelg langeb kokku reaaltelje positiivse suunaga. Igale kompleksarvule $z = a + bi$ vastab komplekstasandil punkt, mille ristkoordinaadid on (a, b). Sellise punkti polaarkoordinaatideks on

1) polaarraadius ehk punkti kaugus r poolusest,

2) polaarnurk ehk nurk φ polaartelje ja vaadeldava punkti kohavektori vahel mõõdetuna kellaosuti liikumise vastassuunas (ehk vastupäeva).

Reaalarvu r nimetatakse kompleksarvu z **mooduliks** ja nurka φ tema **argumendiks**. Kasutatakse tähistusi

$$r = |z| \quad \text{ja} \quad \varphi = \arg(z).$$

Kompleksarvu 0 moodul on 0, aga argument ei ole määratud.

Pythagorase teoreemi põhjal (vt. joonist) on selge, et

$$\boxed{r = \sqrt{a^2 + b^2}.}$$

Arvule z vastava komplekstasandi punkti ristkoordinaatide ja polaarkoordinaatide vahel kehtivad järgmised seosed:

$$\begin{aligned} a &= r\cos\varphi, \\ b &= r\sin\varphi. \end{aligned}$$

Siit näeme, et kui $a \neq 0$ (s.t. kui kompleksarvule vastav punkt ei asu imaginaarteljel), siis

$$\boxed{\tan\varphi = \frac{b}{a}.}$$

Kui $a = 0$ ja $b \neq 0$, siis $\varphi = \frac{\pi}{2}$ või $\varphi = \frac{3\pi}{2}$ sõltuvalt sellest, kas $b > 0$ või $b < 0$.

Samuti võime öelda, et $z = a + bi = r\cos\varphi + i \cdot r\sin\varphi = r(\cos\varphi + i\sin\varphi)$. Kompleksarvu z esitust kujul

$$z = r(\cos\varphi + i\sin\varphi)$$

nimetatakse selle kompleksarvu **trigonomeetriliseks kujuks**.

Arvestades siinus- ja koosinusfunktsiooni perioodilisust võib öelda, et

$$r(\cos\varphi + i\sin\varphi) = r(\cos(\varphi + 2k\pi) + i\sin(\varphi + 2k\pi))$$

iga $k \in \mathbb{Z}$ korral. Seda arvestades on mugav lugeda arvu z trigonomeetriliseks kujuks ka need avaldised, kus φ asemel on $\varphi + 2k\pi$, kus $k \in \mathbb{Z}$. Siis võime öelda, et

$$r_1(\cos\varphi_1 + i\sin\varphi_1) = r_2(\cos\varphi_2 + i\sin\varphi_2) \iff r_1 = r_2 \wedge (\exists k \in \mathbb{Z})(\varphi_1 = \varphi_2 + 2k\pi). \qquad (22)$$

Sõnades: *trigonomeetrilisel kujul antud kompleksarvud on võrdsed parajasti siis, kui nende moodulid on võrdsed ja argumendid erinevad täispöörde täisarvkordse võrra.*

Näide 5.8 Kompleksarvu $z = \frac{3\sqrt{3}}{2} + \frac{3}{2}i$ võib trigonomeetrilisel kujul esitada näiteks järgnevalt:

$$z = 3\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right) = 3\left(\cos\frac{13\pi}{6} + i\sin\frac{13\pi}{6}\right) = 3\left(\cos\left(-\frac{11\pi}{6}\right) + i\sin\left(-\frac{11\pi}{6}\right)\right).$$

Vaatleme, kuidas korrutada trigonomeetrilisel kujul olevaid kompleksarve. Olgu meil arvud $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ ja $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$. Siis

$$\begin{aligned} z_1 z_2 &= r_1 r_2\left[(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\right] \\ &= r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)). \end{aligned}$$

Seega *kompleksarvude korrutise moodul on tegurite moodulite korrutis ja korrutise argument on tegurite argumentide summa*:

$$\boxed{z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).} \tag{23}$$

Kui $z = r(\cos\varphi + i\sin\varphi) \neq 0$, siis

$$z \cdot \left(\frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi))\right) = \frac{r}{r}(\cos(\varphi - \varphi) + i\sin(\varphi - \varphi)) = \cos 0 + i\sin 0 = 1,$$

mis tähendab, et

$$z^{-1} = \frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi)).$$

Järelikult, kasutades eelnevaid tähistusi võime öelda, et $z_2 \neq 0$ korral

$$\boxed{\frac{z_1}{z_2} = z_1 z_2^{-1} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).}$$

Niisiis: *kompleksarvude z_1 ja z_2 jagatise moodul on nende arvude moodulite jagatis ja argument on nende arvude argumentide vahe.*

Kui $z = r(\cos\varphi + i\sin\varphi)$ ja $n \in \mathbb{N}$, siis valemit (23) rakendades saame järgmise valemi kompleksarvu astendamiseks:

$$\boxed{z^n = r^n(\cos n\varphi + i\sin n\varphi).}$$

Seda valemit kutsutakse *Moivre'i*[3] *valemiks.*

5.3 Kompleksarvude juurimine

Definitsioon 5.9 Olgu n naturaalarv. Kompleksarvu w nimetatakse **n-nda astme juureks** kompleksarvust z, kui $w^n = z$.

Kuna nullist erinevate kompleksarvude korrutis ei saa olla null, siis ainsaks n-nda astme juureks kompleksarvust 0 on 0 ise. Edasises tegeleme nullist erinevate kompleksarvude juurte uurimisega. Osutub, et nullist erineval kompleksarvul z võib olla mitu n-nda astme juurt. Tähistame kõigi nende juurte hulka sümboliga $\sqrt[n]{z}$. Kui r on kompleksarvu $z \neq 0$ moodul, siis sümboliga $\sqrt[n]{r}$ tähistame sellist positiivset reaalarvu, mille n-s aste on r.

Teoreem 5.10 *Kui $n \in \mathbb{N}$ ja $z = r(\cos\varphi + i\sin\varphi) \in \mathbb{C} \setminus \{0\}$, siis n-nda astme juuri arvust z on täpselt n tükki ja*

$$\boxed{\sqrt[n]{z} = \left\{ \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right) \,\middle|\, k \in \{0, 1, \ldots, n-1\} \right\}.} \tag{24}$$

Tõestus. Kui võtame suvalise arvu tõestatava võrduse paremal poolel olevast hulgast ja kasutades Moivre'i valemit tõstame selle astmesse n, siis saame arvu z. Seega paremal poolel olev hulk sisaldub hulgas $\sqrt[n]{z}$.

Näitame, et kehtib vastupidine sisalduvus. Olgu $w = s(\cos\psi + i\sin\psi)$ selline kompleksarv, et $w^n = z$. Siis Moivre'i valemi põhjal

$$s^n(\cos n\psi + i\sin n\psi) = r(\cos\varphi + i\sin\varphi).$$

[3] Abraham de Moivre (1667–1754) — prantsuse matemaatik.

Kriteeriumi (22) põhjal $s^n = r$ ja leidub selline $l \in \mathbb{Z}$, et $n\psi = \varphi + 2l\pi$. Järelikult $s = \sqrt[n]{r}$ ja $\psi = \frac{\varphi+2l\pi}{n}$. Jagades arvu l jäägiga arvuga n saame leida sellised $q, k \in \mathbb{Z}$, et $l = qn + k$ ja $0 \leqslant k < n$. Seega

$$\frac{\varphi + 2l\pi}{n} = \frac{\varphi + 2(qn+k)\pi}{n} = \frac{\varphi + 2k\pi}{n} + 2q\pi$$

ja

$$w = \sqrt[n]{r}\left(\cos\frac{\varphi + 2l\pi}{n} + i\sin\frac{\varphi + 2l\pi}{n}\right) = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right),$$

kus $k \in \{0, 1, \ldots, n-1\}$ ja viimase võrduse juures kasutasime siinuse ja koosinuse perioodilisust. Sellega oleme tõestanud nõutud hulkade võrduse.

Näitame lõpuks, et n-nda astme juuri on n tükki. Teame juba, et neid ei saa olla rohkem kui n. Veendume, et neid on vähemalt n. Selleks näitame, et argumentide

$$\frac{\varphi}{n}, \frac{\varphi + 2\pi}{n}, \frac{\varphi + 4\pi}{n}, \ldots, \frac{\varphi + 2(n-1)\pi}{n}$$

hulgas ei ole selliseid, mis erineks täispöörde täisarvkordse võrra. Oletame vastuväiteliselt, et $0 \leqslant k < l \leqslant n-1$ ja

$$2\pi u = \frac{\varphi + 2l\pi}{n} - \frac{\varphi + 2k\pi}{n} = \frac{(l-k)\cdot 2\pi}{n}$$

mingi $u \in \mathbb{Z}$ korral. Järelikult $nu = l - k > 0$, millest saame, et $u \neq 0$. Järelikult $u \geqslant 1$ ja $l - k \geqslant n$, mis on vastuolus eeldusega. □

Valemi (24) põhjal võib geomeetriliselt öelda, et *n-nda astme juured kompleksarvust $z = r(\cos\varphi + i\sin\varphi) \in \mathbb{C} \setminus \{0\}$ asuvad komplekstasandil sellise korrapärase n-nurga tippudes, mille ümberringjoone raadius on $\sqrt[n]{r}$.*

Definitsioon 5.11 **n-nda astme ühejuur** on n-nda astme juur kompleksarvust 1.

Kuna $1 = \cos 0 + i\sin 0$, siis valemi (24) põhjal

$$\boxed{\sqrt[n]{1} = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \;\middle|\; k \in \{0, 1, \ldots, n-1\}\right\}.}$$

Tähistame iga $k \in \mathbb{Z}$ korral

$$\varepsilon_k := \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

ja toome sisse ka tähistuse

$$H_n := \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\} = \sqrt[n]{1}.$$

Kasutades samasugust mõttekäiku nagu oli teoreemi 5.10 tõestuses võime öelda, et

$$H_n = \{\varepsilon_k \mid k \in \mathbb{Z}\}. \tag{25}$$

Paneme veel tähele, et Moivre'i valemist järeldub, et iga $l \in \{0, 1, \ldots, n-1\}$ korral

$$\varepsilon_l = \varepsilon_1^l,$$

s.t. kõik n-nda astme ühejuured avalduvad ε_1 astmetena. Samuti võib öelda, et mistahes $k, l \in \mathbb{Z}$ korral

$$\begin{aligned}\varepsilon_k = \varepsilon_l &\iff (\exists u \in \mathbb{Z})\left(2\pi \cdot u = \frac{2k\pi}{n} - \frac{2l\pi}{n} = \frac{(k-l)\cdot 2\pi}{n}\right)\\ &\iff (\exists u \in \mathbb{Z})(nu = k - l) \iff n \mid k - l \iff k \equiv l \pmod{n}.\end{aligned}$$

Teoreem 5.12 *n-nda astme ühejuurte hulk H_n on rühm kompleksarvude korrutamise suhtes.*

TÕESTUS. Kui $\varepsilon_k, \varepsilon_l \in H_n$, siis ka

$$\varepsilon_k \cdot \varepsilon_l = \cos \frac{2(k+l)\pi}{n} + i \sin \frac{2(k+l)\pi}{n} = \varepsilon_{k+l} \in H_n$$

tänu võrdusele (25), seega korrutamine on algebraline tehe hulgal H_n. Kuna kõigi kompleksarvude korrutamine on assotsiatiivne, siis on seda ka ühejuurte korrutamine. Samuti on ühejuurte korrutamine kommutatiivne. Ühikelemendiks on kompleksarv $1 = \varepsilon_0 \in H_n$. Et mistahes $k \in \mathbb{Z}$ korral

$$\varepsilon_k \cdot \varepsilon_{n-k} = \varepsilon_{k+n-k} = \varepsilon_n = 1,$$

siis $\varepsilon_k^{-1} = \varepsilon_{n-k}$. Seega $(H_n, \cdot)$ on rühm. □

Definitsioon 5.13 Rühmad $(G, *)$ ja $(H, \circ)$ on **isomorfsed**, kui leidub bijektiivne kujutus $f : G \to H$ nii, et

$$f(a * b) = f(a) \circ f(b)$$

mistahes $a, b \in G$ korral.

Lause 5.14 *Rühmad $(H_n, \cdot)$ ja $(\mathbb{Z}_n, +)$ on isomorfsed.*

TÕESTUS. Defineerime kujutuse $f : \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\} \longrightarrow \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ võrdusega

$$f(\varepsilon_k) := \overline{k}.$$

On selge, et see kujutus on sürjektiivne. Kui $\overline{k} = \overline{l}$, siis $\varepsilon_k = \varepsilon_l$, mis tähendab, et f on injektiivne. Olgu $k, l \in \mathbb{Z}$ ja olgu r jääk, mis tekib arvu $k + l$ jagamisel arvuga n. Siis $\varepsilon_{k+l} = \varepsilon_r$ ja

$$f(\varepsilon_k \cdot \varepsilon_l) = f(\varepsilon_{k+l}) = f(\varepsilon_r) = \overline{r} = \overline{k+l} = \overline{k} + \overline{l} = f(\varepsilon_k) + f(\varepsilon_l).$$

□

6 Vektorruum. Lineaarne sõltuvus

Koolist on teada, et nii tasandil kui kolmemõõtmelises ruumis võib vaadelda vabavektoreid. Neid vabavektoreid saab omavahel liita ja arvuga korrutada ning nendel tehetel on terve rida häid omadusi. Nende struktuuride üldistamiseks on lineaaralgebras kasutusele võetud vektorruumi mõiste. Kui vabavektoreid saab korrutada reaalarvudega, siis üldisema vektorruumi elemente saab korrutada korpuse elementidega.

6.1 Vektorruumi mõiste

Definitsioon 6.1 Hulka V nimetatakse **vektorruumiks** ehk **lineaarseks ruumiks** üle korpuse K, kui on defineeritud kujutused $V \times V \to V, (a, b) \mapsto a + b$, ja $K \times V \to V, (k, a) \mapsto ka$, nii et

VR1. $(a + b) + c = a + (b + c)$ iga $a, b, c \in V$ korral;

VR2. leidub element $0 \in V$ nii, et iga $a \in V$ korral $a + 0 = a = 0 + a$;

VR3. iga elemendi $a \in V$ korral leidub element $-a \in V$ nii, et $a + (-a) = 0 = (-a) + a$;

VR4. $a + b = b + a$ iga $a, b \in V$ korral;

VR5. $k(a + b) = ka + kb$ iga $a, b \in V$ ja $k \in K$ korral;

VR6. $(k + l)a = ka + la$ iga $a \in V$ ja $k, l \in K$ korral;

VR7. $(kl)a = k(la)$ iga $a \in V$ ja $k, l \in K$ korral;

VR8. $1a = a$ iga $a \in V$ korral.

Vektorruumi V elemente on tavaks nimetada **vektoriteks** ja korpuse K elemente **skalaarideks**. Elementi $a + b \in V$ nimetatakse vektorite a ja b **summaks** ning elementi $ka \in V$ skalaari k ja vektori a **korrutiseks**. Elementi $0 \in V$ tingimuses VR2 nimetatakse **nullvektoriks** ja elementi $-a \in V$ tingimuses VR3 nimetatakse vektori a **vastandvektoriks**.

Märkus 6.2 Tingimustest VR1-VR4 näeme, et vektorruum on liitmistehte suhtes Abeli rühm.

Märkus 6.3 Matemaatilise induktsiooni abil on lihtne näidata, et kui kehtivad tingimused VR5 ja VR6, siis iga naturaalarvu n ja mistahes $a_1, \ldots, a_n, a \in V$, $k, k_1, \ldots, k_n \in K$ korral

$$\begin{aligned} k(a_1 + \ldots + a_n) &= ka_1 + \ldots + ka_n, \\ (k_1 + \ldots + k_n)a &= k_1a + \ldots + k_na. \end{aligned}$$

Näide 6.4 1. Tasandi vabavektorite hulk $\mathbb{E}_2$ ja kolmemõõtmelise ruumi vabavektorite hulk $\mathbb{E}_3$ on vektorruumid.

2. Iga korpus K on vektorruum üle iseenda, kui kujutused $K \times K \to K$ on selle korpuse liitmis- ja korrutamistehe.

3. Iga korpuse K ja naturaalarvu n korral võib hulka K^n vaadelda vektorruumina üle K, kui tehted defineerida n.ö. komponenthaaval:

$$\begin{aligned} (k_1, \ldots, k_n) + (l_1, \ldots, l_n) &:= (k_1 + l_1, \ldots, k_n + l_n), \\ k(k_1, \ldots, k_n) &:= (kk_1, \ldots, kk_n) \end{aligned}$$

mistahes $k, k_1, \ldots, k_n, l_1, \ldots, l_n \in K$ korral.

4. $(m \times n)$-maatriksite hulk $\mathrm{Mat}_{m,n}(K)$ üle korpuse K on vektorruum üle K, kui tehetena vaadelda maatriksite liitmist ja maatriksi korrutamist korpuse K elementidega. See on tõestatud lauses 1.24. Vektorruum K^n on sisuliselt sama, mis $\mathrm{Mat}_{1,n}(K)$.

5. Hulk $\mathbb{C}$ on vektorruum üle korpuse $\mathbb{R}$, kui liitmisena vaadelda kompleksarvude liitmist ning reaalarvu c ja kompleksarvu $a + bi$ korrutis defineeritakse kui $c(a + bi) := ca + cbi$.

Lause 6.5 *Mistahes vektorruumis V üle suvalise korpuse K kehtivad järgmised arvutusreeglid.*

1. *Iga $a, b, c \in V$ korral, kui $a + b = c$, siis $a = c - b$.*
2. *$0a = 0$ iga $a \in V$ korral. (Selle võrduse vasakul poolel olev 0 tähistab korpuse K nullelementi ja paremal poolel olev 0 vektorruumi V nullelementi.)*
3. *$k0 = 0$ iga $k \in K$ korral. (Selles võrduses on mõlemad 0-d V elemendid.)*
4. *$(-1)a = -a$ iga $a \in V$ korral. (Siin -1 on korpuse K ühikelemendi vastandelement.)*
5. *$(-k)a = k(-a) = -(ka)$ iga $k \in K$ ja $a \in V$ korral.*
6. *$k(a - b) = ka - kb$ iga $k \in K$ ja $a, b \in V$ korral.*
7. *$(k - l)a = ka - la$ iga $k, l \in K$ ja $a \in V$ korral.*

Tõestus. Kõik need omadused saab tõestada väga sarnaselt sellele, kuidas on tõestatud ringide kohta käiv lause 4.17. □

6.2 Vektorruumi alamruum

Algebras kutsutakse algebralise struktuuri mittetühje tehete suhtes kinniseid alamhulki alamstruktuurideks. Nii võib rääkida näiteks alamrühmadest, alamringidest ja alamkorpustest. Meie uurime põhjalikumalt vektorruumide alamstruktuure.

Definitsioon 6.6 Vektorruumi V mittetühja alamhulka U nimetatakse V **alamruumiks**, kui

AR1 iga $a, b \in U$ korral $a + b \in U$ (s.t. U on kinnine liitmise suhtes);

AR2 iga $a \in U$ ja $k \in K$ korral $ka \in U$ (s.t. U on kinnine skalaariga korrutamise suhtes).

Näide 6.7 1. Iga vektorruumi V korral on V ise ja nullvektorist koosnev alamhulk $\{0\}$ selle vektorruumi alamruumid.

2. Mistahes korpuse K ja naturaalarvu n korral on n-ndat järku sümmeetriliste maatriksite (üle K) hulk alamruum vektorruumis $\mathrm{Mat}_n(K)$.

3. Hulk $U = \{(k, 0, l) \mid k, l \in \mathbb{R}\}$ on alamruum vektorruumis $\mathbb{R}^3$ (üle korpuse $\mathbb{R}$).

4. Fikseeritud sirgega paralleelsete vabavektorite hulk on alamruum tasandi vabavektorite vektorruumis $\mathbb{E}_2$.

Lause 6.8 *Vektorruumi iga alamruum sisaldab nullvektorit.*

Tõestus. Olgu U vektorruumi V alamruum. Kuna U on mittetühi, siis leidub mingi $a \in U$. Tingimuse AR2 ja lause 6.5(2) tõttu $0 = 0a \in U$. □

Lause 6.9 *Vektorruumi V iga alamruum on ise ka vektorruum tehete suhtes, mis on defineeritud samamoodi nagu vektorruumi V tehted.*

TÕESTUS. Olgu U vektorruumi V alamruum. Tingimused AR1 ja AR2 tagavad selle, et võime vaadelda kujutusi $U \times U \to U$, $(a, b) \mapsto a+b$, ja $K \times U \to U$, $(k, a) \mapsto ka$. On selge, et tingimused VR1 ja VR4-VR8 on U korral täidetud. Lausest 6.8 järeldub, et ka tingimus VR2 kehtib U jaoks. Kui $a \in U$, siis lause 6.5 põhjal võib öelda, et $(-1)a = -a$. Kuna AR2 tõttu $(-1)a \in U$, siis ka $-a \in U$. Seega U rahuldab tingimust VR3. □

Definitsioon 6.10 Olgu V vektorruum üle korpuse K ja $a_1, \ldots, a_s \in V$. Mistahes avaldist

$$k_1a_1 + k_2a_2 + \ldots + k_sa_s, \tag{26}$$

kus $k_1, \ldots, k_s \in K$, aga ka selle avaldise poolt määratud V elementi, nimetatakse vektorite $a_1, \ldots, a_s$ **lineaarkombinatsiooniks.** Skalaare $k_1, \ldots, k_s$ nimetatakse selle lineaarkombinatsiooni **kordajateks**.

Näide 6.11 Olgu $a = (3, -1, 2)$ ja $b = (1, 4, 0)$ vektorruumi $\mathbb{R}^3$ vektorid ning $k = 2$ ja $l = 3$. Arvutame lineaarkombinatsiooni $ka + lb$:

$$ka + lb = 2 \cdot (3, -1, 2) + (-3) \cdot (1, 4, 0) = (6, -2, 4) + (-3, -12, 0) = (3, -14, 4).$$

Definitsioon 6.12 Vektorruumi V alamhulka, mis koosneb vektorite $a_1, \ldots, a_s$ kõigist lineaarkombinatsioonidest, nimetatakse vektorite $a_1, \ldots, a_s$ **lineaarseks katteks** ehk **lineaarkatteks** ja tähistatakse kas $L(a_1, \ldots, a_s)$ või $\langle a_1, \ldots, a_s \rangle$.

Seega

$$L(a_1, \ldots, a_s) = \{k_1a_1 + \ldots + k_sa_s \mid k_1, \ldots, k_s \in K\}.$$

Lineaarkatete moodustamine annab ühe kasuliku viisi alamruumide konstrueerimiseks.

Lause 6.13 *Vektorite $a_1, \ldots, a_s$ lineaarne kate on vähim alamruum, mis neid vektoreid sisaldab.*

TÕESTUS. Olgu $a_1, \ldots, a_s$ vektorruumi V (üle korpuse K) vektorid. Kuna $0 = 0a_1 + \ldots + 0a_s \in L(a_1, \ldots, a_s)$, siis $L(a_1, \ldots, a_s)$ ei ole tühi. Kui $k_1a_1 + \ldots + k_sa_s, l_1a_1 + \ldots + l_sa_s \in L(a_1, \ldots, a_s)$ ja $k \in K$, siis

$$\begin{aligned}(k_1a_1 + \ldots + k_sa_s) + (l_1a_1 + \ldots + l_sa_s) &= (k_1 + l_1)a_1 + \ldots + (k_s + l_s)a_s \in L(a_1, \ldots, a_s),\\ k(k_1a_1 + \ldots + k_sa_s) &= (kk_1)a_1 + \ldots + (kk_s)a_s \in L(a_1, \ldots, a_s).\end{aligned}$$

Sellega oleme näidanud, et $L(a_1, \ldots, a_s)$ on V alamruum. Et

$$a_i = 0a_1 + \ldots + 0a_{i-1} + 1a_i + 0a_{i+1} + \ldots + 0a_n \in L(a_1, \ldots, a_s)$$

iga $i \in \{1, \ldots, n\}$ korral, siis $L(a_1, \ldots, a_s)$ sisaldab vektoreid $a_1, \ldots, a_s$. Kui U on mistahes alamruum, mis sisaldab vektoreid $a_1, \ldots, a_s$, siis ta peab sisaldama ka kõiki vektoreid $k_1a_1, \ldots, k_sa_s$, kus $k_1, \ldots, k_s \in K$, ning ka selliste vektorite summasid. Seega $L(a_1, \ldots, a_s) \subseteq U$, s.t. $L(a_1, \ldots, a_s)$ on vähim V alamruum, mis sisaldab vektoreid $a_1, \ldots, a_s$. □

Näide 6.14 Vektorruumi $\mathbb{R}^3$ vektorite $a = (1, 0, 0)$ ja $b = (0, 0, 1)$ lineaarne kate on alamruum $L(a, b) = \{(k, 0, l) \mid k, l \in \mathbb{R}\}$.

6.3 Lineaarne sõltumatus

Vektoritest rääkides kasutatakse tihti terminit **vektorite süsteem**. Selle all mõeldakse sellist vektorite kogumit, mis erineb vektorite hulgast selle poolest, et üks vektor võib selles esineda mitu korda. Samuti on vektorite süsteemi puhul oluline vektorite järjekord. Näiteks kui V on vektorruum ja $a, b, c \in V$, siis võib vaadelda vektorite süsteemi c, a, b, a, c. Käesolevas kursuses vaatleme vaid lõplikke vektorite süsteeme. Formaalselt võib vektorite süsteemi $a_1, a_2, \ldots, a_s$ vaadelda hulga V^s elemendina, kus $s \in \mathbb{N}$. Harilikult seda vaatepunkti siiski ei rõhutata.

Anname nüüd lineaarse sõltumatuse definitsiooni.

Definitsioon 6.15 Vektorruumi V (üle korpuse K) vektorite süsteemi $a_1, a_2, \ldots, a_s$ nimetatakse **lineaarselt sõltumatuks**, kui mistahes $k_1, k_2, \ldots, k_s \in K$ korral võrdusest

$$k_1a_1 + k_2a_2 + \ldots + k_sa_s = 0$$

järeldub, et

$$k_1 = k_2 = \ldots = k_s = 0.$$

Vektorite süsteemi nimetatakse **lineaarselt sõltuvaks**, kui ta ei ole lineaarselt sõltumatu.

Niisiis vektorite süsteem $a_1, a_2, \ldots, a_s$ on lineaarselt sõltuv, kui leiduvad sellised skalaarid $k_1, k_2, \ldots, k_s \in K$, et

$$k_1a_1 + k_2a_2 + \ldots + k_sa_s = 0$$

ja vähemalt üks elementidest $k_1, k_2, \ldots, k_s$ on nullist erinev.

Definitsioon 6.16 Lineaarkombinatsiooni nimetatakse **triviaalseks**, kui kõik tema kordajad on nullid. Kui vähemalt üks kordaja on nullist erinev, siis öeldakse, et see lineaarkombinatsioon on **mittetriviaalne**.

Seega lineaarse sõltumatuse definitsiooni võib anda ka järgmisel kujul: vektorite süsteem on lineaarselt sõltumatu, kui nullvektoriga on võrdne vaid selle süsteemi triviaalne lineaarkombinatsioon. Vektorite süsteem on lineaarselt sõltuv, kui mingi mittetriviaalne lineaarkombinatsioon selle süsteemi vektoritest on võrdne nullvektoriga.

Näide 6.17 Vektorruumi $\mathbb{R}^3$ vektorite süsteem

$$\begin{aligned} a_1 &= (1, 1, -2), \\ a_2 &= (-2, -2, 4) \end{aligned}$$

on lineaarselt sõltuv, sest $2a_1 + a_2 = (0, 0, 0)$. Süsteem

$$\begin{aligned} b_1 &= (1, 0, 0), \\ b_2 &= (0, 2, 0), \\ b_3 &= (0, 0, 4) \end{aligned}$$

on aga lineaarselt sõltumatu, sest kui

$$(0, 0, 0) = k_1b_1 + k_2b_2 + k_3b_3 = (k_1, 0, 0) + (0, 2k_2, 0) + (0, 0, 4k_3) = (k_1, 2k_2, 4k_3),$$

siis $0 = k_1 = 2k_2 = 4k_3$, millest $0 = k_1 = k_2 = k_3$. Analoogiliselt saab näidata, et mistahes järku ühikmaatriksi reavektorite süsteem on lineaarselt sõltumatu.

Märkus 6.18 Kuna vektorruumi liitmistehe on kommutatiivne, siis vektorite süsteemi lineaarne sõltuvus või sõltumatus ei sõltu vaadeldavate vektorite järjestusest.

Tuleb välja, et lisaks definitsioonile on veel terve rida tingimusi, mille abil saab otsustada vektorite süsteemi lineaarse sõltuvuse või sõltumatuse üle. Järgnevas vaatleme neist mõningaid.

Lause 6.19 *Ühestainsast vektorist a koosnev süsteem on lineaarselt sõltumatu parajasti siis, kui $a \neq 0$.*

Tõestus. Tarvilikkus. Olgu vektorist a koosnev süsteem lineaarselt sõltumatu. Kui oletame, et $a = 0$ ja võtame näiteks korpuse ühikelemendi 1, siis lause 6.5(3) põhjal $1a = 0 \in V$, mis on vastuolus süsteemi lineaarse sõltumatusega. Järelikult $a \neq 0$.
Piisavus. Olgu $a \neq 0$. Oletame, et $ka = 0$, kus k on korpuse element. Kui $k \neq 0$, siis leidub pöördelement k^{-1}. Korrutades sellega võrduse $ka = 0$ pooli saame

$$0 \underset{lause\ 6.5(3)}{=} k^{-1}0 = k^{-1}(ka) \underset{VR7}{=} (k^{-1}k)a = 1a \underset{VR8}{=} a,$$

mis on vastuolus eeldusega. Järelikult $k = 0$. Definitsiooni põhjal on vektorist a koosnev süsteem lineaarselt sõltumatu. □

Lause 6.20 *Vektorite süsteem $a_1, \ldots, a_s$, kus $s \geqslant 2$, on lineaarselt sõltuv parajasti siis, kui selles süsteemis leidub vektor, mis avaldub ülejäänud vektorite lineaarkombinatsioonina.*

Tõestus. Tarvilikkus. Olgu süsteem $a_1, \ldots, a_s$, kus $s \geqslant 2$, lineaarselt sõltuv. Siis

$$k_1a_1 + \ldots + k_sa_s = 0$$

mingite elementide $k_1, \ldots, k_s \in K$ korral, kusjuures vähemalt üks neist — olgu see k_i — on nullist erinev. Siis

$$k_ia_i = -k_1a_1 - \ldots - k_{i-1}a_{i-1} - k_{i+1}a_{i+1} - \ldots - k_sa_s. \tag{27}$$

Kuna $k_i \neq 0$, siis leidub tal pöördelement $k_i^{-1} \in K$. Korrutades võrduse (27) mõlemaid pooli elemendiga k_i^{-1} saame võrduse

$$a_i = k_i^{-1}(k_ia_i) = -k_i^{-1}k_1a_1 - \ldots - k_i^{-1}k_{i-1}a_{i-1} - k_i^{-1}k_{i+1}a_{i+1} - \ldots - k_i^{-1}k_sa_s.$$

See tähendab, et vektor a_i avaldub ülejäänud vektorite lineaarkombinatsioonina.
Piisavus. Oletame, et vektor a_i avaldub ülejäänud vektorite lineaarkombinatsioonina:

$$a_i = l_1a_1 + \ldots + l_{i-1}a_{i-1} + l_{i+1}a_{i+1} + \ldots + l_sa_s,$$

kus $l_1, \ldots, l_{i-1}, l_{i+1}, \ldots, l_s \in K$. Siis

$$l_1a_1 + \ldots + l_{i-1}a_{i-1} + (-1)a_i + l_{i+1}a_{i+1} + \ldots + l_sa_s = 0,$$

kusjuures lineaarkombinatsioon viimase võrduse vasakul poolel on mittetriviaalne, sest a_i kordaja ei ole 0. Järelikult on süsteem $a_1, \ldots, a_s$ lineaarselt sõltuv. □

Järeldus 6.21 *Vektorite süsteem $a_1, \ldots, a_s$, kus $s \geqslant 2$, on lineaarselt sõltumatu parajasti siis, kui selle süsteemi ükski vektor ei avaldu ülejäänud vektorite lineaarkombinatsioonina.*

Järeldus 6.22 *Kahest vektorist koosnev süsteem on lineaarselt sõltuv parajasti siis, kui üks vektor on teisest saadav skalaariga korrutades.*

Järeldus 6.23 *Iga vektorite süsteem, mis sisaldab kahte võrdset vektorit, on lineaarselt sõltuv.*

Järeldus 6.24 *Iga vektorite süsteem, mis sisaldab nullvektorit, on lineaarselt sõltuv.*

TÕESTUS. Kui nullvektor on süsteemi ainus vektor, siis on see süsteem lineaarselt sõltuv tänu lausele 6.19. Kui süsteemis on vähemalt kaks vektorit, siis nullvektor avaldub ülejäänud vektorite triviaalse lineaarkombinatsioonina. Seega süsteem on lineaarselt sõltuv lause 6.20 põhjal. □

Lause 6.25 *Kui vektorite süsteemi mingi alamsüsteem on lineaarselt sõltuv, siis ka terve süsteem on lineaarselt sõltuv.*

TÕESTUS. Kuna vektorite järjekorra muutmine ei muuda süsteemi lineaarset sõltuvust/sõltumatust, siis võime eeldada, et süsteemi $a_1, \ldots, a_s$ lineaarselt sõltuv alamsüsteem koosneb selle süsteemi t ($t \leqslant s$) esimesest vektorist $a_1, \ldots, a_t$. Siis leiduvad $k_1, \ldots, k_t \in K$, millest vähemalt üks on nullist erinev, nii et

$$k_1a_1 + \ldots + k_ta_t = 0.$$

Siis kehtib ka võrdus

$$k_1a_1 + \ldots + k_ta_t + 0a_{t+1} + \ldots + 0a_s = 0,$$

kusjuures viimase võrduse vasakul poolel on mittetriviaalne lineaarkombinatsioon vektoritest $a_1, \ldots, a_s$. Järelikult on süsteem $a_1, \ldots, a_s$ lineaarselt sõltuv. □

Lause 6.26 *Lineaarselt sõltumatu vektorite süsteemi iga alamsüsteem on ka lineaarselt sõltumatu.*

TÕESTUS. Olgu süsteem $a_1, \ldots, a_s$ lineaarselt sõltumatu. Kui selle süsteemi mingi alamsüsteem $a_{i_1}, \ldots, a_{i_t}$ oleks lineaarselt sõltuv, siis lause 6.25 põhjal oleks ka $a_1, \ldots, a_s$ lineaarselt sõltuv, mis on vastuolus eeldusega. Seega on kõik alamsüsteemid lineaarselt sõltumatud. □

Lause 6.27 *Nullist erinevate vektorite süsteem $a_1, \ldots, a_s$, kus $s \geqslant 2$, on lineaarselt sõltuv parajasti siis, kui leidub vektor, mis avaldub eelnevate vektorite lineaarkombinatsioonina.*

TÕESTUS. Vaatleme nullist erinevate vektorite süsteemi $a_1, \ldots, a_s$, kus $s \geqslant 2$, vektoruumis V üle korpuse K.
TARVILIKKUS. Olgu süsteem $a_1, \ldots, a_s$ lineaarselt sõltuv. Siis leiduvad $k_1, \ldots, k_s \in K$, mis ei ole kõik nullid, nii et

$$k_1a_1 + \ldots + k_sa_s = 0.$$

Olgu k_l viimane nullist erinev kordaja eelmise võrduse vasakul poolel. Siis

$$k_1a_1 + \ldots + k_la_l = 0$$

Paneme tähele, et $l \neq 1$. Tõepoolest, kui $l = 1$, siis $k_1a_1 = 0$, millest elemendiga k_1^{-1} korrutades saame $a_1 = 0$. Viimane on vastuolus eeldusega. Niisiis $l > 1$. Kasutades arvutusreegleid vektorruumis saame avaldada

$$a_l = -k_l^{-1}k_1a_1 - \ldots - k_l^{-1}k_{l-1}a_{1-1},$$

mis tähendab, et a_l on talle eelnevate vektorite $a_1, \ldots, a_{l-1}$ lineaarkombinatsioon.
PIISAVUS. Oletame, et vektor a_l avaldub eelnevate vektorite lineaarkombinatsioonina:

$$a_l = k_1 a_1 + \ldots + k_{l-1} a_{l-1},$$

kus $k_1, \ldots, k_{l-1} \in K$. Liites selle võrduse mõlemale poolele vektori $-a_l$ saame võrduse

$$k_1 a_1 + \ldots + k_{l-1} a_{l-1} + (-1) a_l + 0 a_{l+1} + \ldots + 0 a_s = 0.$$

Siit näeme, et süsteem $a_1, \ldots, a_s$ on lineaarselt sõltuv. □

Järeldus 6.28 *Nullist erinevate vektorite süsteem $a_1, \ldots, a_s$, kus $s \geqslant 2$, on lineaarselt sõltumatu parajasti siis, kui selle süsteemi ükski vektor ei avaldu eelnevate vektorite lineaarkombinatsioonina.*

Näide 6.29 Tänu järeldusele 6.28 on näiteks selge, et vektorruumi $\mathbb{R}^4$ vektorite süsteem

$$\begin{aligned} a_1 &= (3,0,0,0), \\ a_2 &= (5,2,1,0), \\ a_3 &= (0,4,0,2) \end{aligned}$$

on lineaarselt sõltumatu.

6.4 Moodustajate süsteem

Definitsioon 6.30 Vektorruumi V vektorite süsteemi M nimetatakse **moodustajate süsteemiks** ehk **tekitajate süsteemiks**, kui vektorruumi V iga vektor avaldub süsteemi M kuuluvate vektorite lineaarkombinatsioonina.

Enamasti on vektorruumil palju moodustajate süsteeme, mõned neist suuremad, mõned väiksemad. Eriti kasulikud on moodustajate süsteemid, mille kaudu iga vektori saab avaldada täpselt ühel viisil. Neid me uurida soovimegi.

Lepime kokku, et **edasises vaatleme selle kursuse jooksul ainult selliseid vektorruume, millel on olemas lõplik moodustajate süsteem.** Vastavalt definitsioonidele võime öelda, et süsteem $a_1, \ldots, a_s$ on vektorruumi V moodustajate süsteem parajasti siis, kui V on selle süsteemi lineaarne kate:

$$V = L(a_1, \ldots, a_s).$$

Alustuseks tõestame ühe abitulemuse.

Lemma 6.31 *Olgu $a_1, \ldots, a_s$ vektorruumi V moodustajate süsteem. Kui selle süsteemi mingi vektor avaldub ülejäänud vektorite lineaarkombinatsioonina, siis selle vektori väljajätmisel süstemist $a_1, \ldots, a_s$ saame jällegi V moodustajate süsteemi.*

TÕESTUS. Oletame, et vektor a_1 avaldub lineaarkombinatsioonina

$$a_1 = k_2 a_2 + \ldots + k_s a_s,$$

kus $k_2, \ldots, k_s \in K$. (Kui ülejäänute kaudu avaldub mõni teine vektor, on tõestus analoogiline.) Olgu nüüd $a \in V$ suvaline vektor. Et $a_1, \ldots, a_s$ on moodustajate süsteem, siis leiduvad sellised $l_1, \ldots, l_s \in K$, et

$$a = l_1 a_1 + l_2 a_2 + \ldots + l_s a_s.$$

Asendades viimasesse võrdusse a_1 avaldise ja kasutades vektorruumi omadusi saame, et

$$a = l_1(k_2a_2 + \ldots + k_sa_s) + l_2a_2 + \ldots + l_sa_s = (l_1k_2 + l_2)a_2 + \ldots + (l_1k_s + l_s)a_s,$$

s.t. a avaldub vektorite $a_2, \ldots, a_s$ lineaarkombinatsioonina. Seega $a_2, \ldots, a_s$ on ka moodustajate süsteem. □

Kuna süsteem $a_1, \ldots, a_n$ on lineaarse katte $L(a_1, \ldots, a_n)$ moodustajate süsteem, siis saame eelmisest lemmast teha järgmise järelduse.

Järeldus 6.32 *Kui vektor a_i, kus $i \in \{1, \ldots, n\}$, avaldub süsteemi $a_1, \ldots, a_n$ ülejäänud vektorite lineaarkombinatsioonina, siis*

$$L(a_1, \ldots, a_n) = L(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n).$$

Näiteks $L(a, b, a, c, b, b) = L(a, b, c)$ mistahes vektorite $a, b, c \in V$ korral.

6.5 Vektorruumi baas

Definitsioon 6.33 Vektorruumi **baas** on selle vektorruumi lineaarselt sõltumatu moodustajate süsteem.

Kuna baasis ei saa ükski vektor esineda kaks korda (muidu oleks süsteem järelduse 6.23 tõttu lineaarselt sõltuv), siis baasivektorid moodustavad hulga. Baasidest rääkides kasutamegi vastavat tähistust, nt. kirjutame

$$e = \{e_1, \ldots, e_n\},$$

kui räägime baasist e, mis koosneb vektoritest $e_1, \ldots, e_n$. Nii nagu kõigi vektorite süsteemide korral on ka baasi puhul vektorite järjekord oluline ja me loeme, et e_1 on baasi e esimene vektor, e_2 on teine vektor jne.

Näide 6.34 1. Vektorruumi K^n vektorite süsteem

$$\begin{aligned} e_1 &= (1, 0, 0, \ldots, 0, 0), \\ e_2 &= (0, 1, 0, \ldots, 0, 0), \\ &\ldots \\ e_n &= (0, 0, 0, \ldots, 0, 1) \end{aligned}$$

on baas. Tõepoolest, kui oletame, et

$$\begin{aligned} (0, 0, \ldots, 0) &= k_1e_1 + k_2e_2 + \ldots + k_ne_n \\ &= k_1(1, 0, \ldots, 0) + k_2(0, 1, \ldots, 0) + \ldots + k_n(0, 0, \ldots, 1) \\ &= (k_1, 0, \ldots, 0) + (0, k_2, \ldots, 0) + \ldots + (0, 0, \ldots, k_n) \\ &= (k_1, k_2, \ldots, k_n), \end{aligned}$$

siis $k_1 = k_2 = \ldots = k_n = 0$, mis tähendab, et süsteem $e_1, e_2, \ldots, e_n$ on lineaarselt sõltumatu. Samuti, iga vektor $(l_1, l_2, \ldots, l_n) \in K^n$ on avaldatav lineaarkombinatsioonina

$$(l_1, l_2, \ldots, l_n) = l_1e_1 + l_2e_2 + \ldots + l_ne_n$$

ja seega $e_1, e_2, \ldots, e_n$ on moodustajate süsteem.

2. Eelneva põhjal teame, et $e_1 = (1,0), e_2 = (0,1)$ on baas vektorruumis $\mathbb{R}^2$. Toome näite ühest teistsugusest $\mathbb{R}^2$ baasist. Vaatleme näiteks vektorite süsteemi

$$\begin{aligned} f_1 &= (1,1), \\ f_2 &= (0,1). \end{aligned}$$

Kui $(0,0) = k_1 f_1 + k_2 f_2 = (k_1, k_1) + (0, k_2) = (k_1, k_1 + k_2)$, siis $k_1 = 0$ ja $k_1 + k_2 = 0$, millest saame, et ka $k_2 = 0$. Seega f_1, f_2 on lineaarselt sõltumatu süsteem. Mistahes vektori $(l_1, l_2) \in \mathbb{R}^2$ saame avaldada kujul

$$(l_1, l_2) = l_1 f_1 + (l_2 - l_1) f_2,$$

s.t. f_1, f_2 on moodustajate süsteem. Järelikult f_1, f_2 on baas.

3. Vektorruumis $\mathbb{E}_2$ moodustavad baasi mistahes 2 mittekollineaarset vektorit.

Teoreem 6.35 *Kui vektorruumis on vähemalt kaks vektorit, siis on selles vektorruumis olemas baas.*

TÕESTUS. Olgu $a_1, \ldots, a_s$ vektorruumi V moodustajate süsteem. (Me oleme eeldanud, et vaadeldavates vektorruumides leidub lõplik moodustajate süsteem.) Et vektorruumis on vähemalt kaks vektorit, siis leidub selles vähemalt üks nullist erinev vektor x. Kui kõik vektorid $a_1, \ldots, a_s$ oleks nullvektorid, siis me ei saaks vektorit x selle süsteemi kaudu avaldada ja see ei oleks moodustajate süsteem. Seega on selles süsteemis vähemalt üks nullist erinev vektor a_i. Kui süsteemis $a_1, \ldots, a_s$ sisaldub nullvektor, siis avaldub see ülejäänud vektorite lineaarkombinatsioonina ja nullvektorit välja jättes saame lemma 6.31 põhjal ikkagi V moodustajate süsteemi. Seega võime üldisust kitsendamata eeldada, et süsteemis $a_1, \ldots, a_s$ ei ole nullvektoreid.

Konstrueerime nüüd süsteemi $a_1, \ldots, a_s$ põhjal uue süsteemi (selle süsteemi alamsüsteemi), mis oleks V baasiks. Selleks jätame vaadeldavast süsteemist $a_1, \ldots, a_s$ välja n.ö. mittevajalikud vektorid. Täpsemalt toimime järgmiselt. Vaatleme vektorit a_2. Kui see vektor avaldub talle eelneva vektori a_1 lineaarkombinatsioonina, siis jätame selle süsteemist välja. Lemma 6.31 tõttu on saadav süsteem ka moodustajate süsteem. Kui a_2 ei avaldu vektori a_1 lineaarkombinatsioonina, siis me teda välja ei jäta. Edasi vaatleme saadud süsteemis vektorit a_3. Kui a_3 avaldub talle eelnevate vektorite lineaarkombinatsioonina, siis jätame selle vektori süsteemist välja. Pärast a_3 vaatlemist on meil ikkagi tegemist moodustajate süsteemiga. Niimoodi jätkates jõuame lõpuks viimase vektorini. Vastavalt konstruktsioonile on lõpuks saadud süsteem $S = \{a_1, a_{i_2}, \ldots, a_{i_n}\}$ (selles süsteemis ei esine ükski vektor kaks korda!) vektorruumi V moodustajate süsteem. Konstruktsiooni põhjal ei avaldu süsteemi S ükski vektor eelnevate vektorite lineaarkombinatsioonina, mis järelduse 6.28 põhjal tähendab, et S on lineaarselt sõltumatu. Kokkuvõttes võime öelda, et S on baas. □

Märkus 6.36 Kui vektorruum koosneb ainult ühest vektorist, siis see vektor on nullvektor. Sellises vektorruumis ei ole baasi, sest ei ole lineaarselt sõltumatuid vektorite süsteeme.

Lause 6.37 *Iga lõpliku mittetühja lineaarselt sõltumatu vektorite süsteemi saab täiendada vektorruumi baasiks.*

TÕESTUS. Olgu $a_1, \ldots, a_k$ ($k \in \mathbb{N}$) lineaarselt sõltumatu vektorite süsteem vektorruumis V ja olgu $e_1, \ldots, e_n$ selle vektorruumi baas. Siis süsteem

$$a_1, \ldots, a_k, e_1, \ldots, e_n$$

on moodustajate süsteem vektorruumis V. Eraldame sellest välja baasi kasutades teoreemi 6.35 tõestuses kirjeldatud meetodit. Siis saadav baas sisaldab kindlasti vektoreid $a_1, \ldots, a_k$, sest ükski neist ei avaldu eelnevate vektorite lineaarkombinatsioonina. □

Meie järgmiseks eesmärgiks on anda veel kaks kirjeldust baasidele.

Definitsioon 6.38 Vektorruumi V vektorite süsteemi S nimetatakse **maksimaalseks lineaarselt sõltumatuks süsteemiks**, kui see süsteem on lineaarselt sõltumatu, aga iga süsteem, mis saadakse süsteemist S ühe vektori lisamisel, on lineaarselt sõltuv.

Definitsioon 6.39 Vektorruumi V vektorite süsteemi S nimetatakse **minimaalseks moodustajate süsteemiks**, kui see süsteem on moodustajate süsteem, aga iga süsteem, mis saadakse süsteemist S ühe vektori väljajätmisel, ei ole moodustajate süsteem.

Teoreem 6.40 *Vektorruumi V (üle korpuse K) lõpliku vektorite süsteemi S korral on järgmised väited samaväärsed.*

1. *S on baas.*
2. *S on maksimaalne lineaarselt sõltumatu süsteem.*
3. *S on minimaalne moodustajate süsteem.*

Tõestus. 1. $\Rightarrow$ 2. Olgu süsteem $e_1, \ldots, e_n$ baas, s.t. lineaarselt sõltumatu moodustajate süsteem. Kui võtame suvalise vektori $a \in V$, siis a avaldub süsteemi $e_1, \ldots, e_n$ lineaarkombinatsioonina. Seega süsteem $e_1, \ldots, e_n, a$ on lause 6.27 põhjal lineaarselt sõltuv. Järelikult $e_1, \ldots, e_n$ on maksimaalne lineaarselt sõltumatu süsteem.

2. $\Rightarrow$ 1. Olgu $e_1, \ldots, e_n$ maksimaalne lineaarselt sõltumatu süsteem. Peame näitama, et see on moodustajate süsteem. Selleks võtame suvalise $a \in V$ ja vaatleme süsteemi

$$e_1, \ldots, e_n, a.$$

Eelduse põhjal on see süsteem lineaarselt sõltuv. Järelikult leidub selles süsteemis vektor, mis avaldub eelnevate lineaarkombinatsioonina. Kuna see ei saa olla ükski vektoritest $e_1, \ldots, e_n$ (muidu oleks süsteem $e_1, \ldots, e_n$ lineaarselt sõltuv), siis see vektor peab olema a. Sellega oleme näidanud, et $e_1, \ldots, e_n$ on moodustajate süsteem.

1. $\Rightarrow$ 3. Olgu süsteem $e_1, \ldots, e_n$ baas. Siis $e_1, \ldots, e_n$ on moodustajate süsteem. Näitame, et süsteem $e_2, \ldots, e_n$ ei ole moodustajate süsteem. (Kui süsteemist jätta välja mõni teine vektor, on tõestus analoogiline.) Kui $e_2, \ldots, e_n$ oleks moodustajate süsteem, siis peaks e_1 avalduma $e_2, \ldots, e_n$ kaudu, mis on vastuolus $e_1, \ldots, e_n$ lineaarse sõltumatusega (vt. järeldust 6.21).

3. $\Rightarrow$ 1. Olgu $e_1, \ldots, e_n$ minimaalne moodustajate süsteem. Peame näitama, et see süsteem on lineaarselt sõltumatu. Kui näiteks $e_1 = k_2e_2 + \ldots + k_se_s$, siis avaldub iga $a \in V$ kujul

$$a = l_1e_1 + l_2e_2 + \ldots + l_se_s = l_1(k_2e_2 + \ldots + k_se_s) + l_2e_2 + \ldots + l_se_s \in L(e_2, \ldots, e_s),$$

mis tähendab, et ka $e_2, \ldots, e_s$ on moodustajate süsteem. Samamoodi saame vastuolu eeldusega, kui mõni teine vektor süsteemis $e_1, \ldots, e_n$ avaldub ülejäänute kaudu. Järelikult $e_1, \ldots, e_n$ on lineaarselt sõltumatu järelduse 6.21 põhjal. □

Tuleb välja, et vektorite arv baasis ei sõltu baasi valikust.

Teoreem 6.41 *Vektorruumi mistahes kahes baasis on samapalju vektoreid.*

TÕESTUS. Kui $V = \{0\}$, siis selles vektorruumis baase ei ole ja seega väide kehtib. Oletame nüüd, et vektorruumis V on vähemalt kaks vektorit. Olgu $A = \{a_1, \ldots, a_m\}$ ja $B = \{b_1, \ldots, b_n\}$ vektorruumi V kaks baasi. Oletame vastuväiteliselt, et $m < n$. Vaatleme süsteemi

$$b_1, a_1, a_2, \ldots, a_m. \tag{T_1}$$

Et baas $a_1, \ldots, a_m$ on maksimaalne lineaarselt sõltumatu süsteem, siis on süsteem (T_1) lineaarselt sõltuv. Seega lause 6.27 põhjal peab süsteemi (T_1) mingi vektor avalduma eelnevate lineaarkombinatsioonina. See peab olema üks vektoritest $a_1, \ldots, a_m$, sest vektorile b_1 ei eelne ühtegi vektorit. Eeldame, et see vektor on a_m (vajaduse korral võime vektorid $a_1, \ldots, a_m$ ümber nummerdada). Kasutades järeldust 6.32 võime kirjutada, et

$$V = L(a_1, \ldots, a_m) = L(b_1, a_1, \ldots, a_{m-1}, a_m) = L(b_1, a_1, \ldots, a_{m-1}).$$

Viimane võrdus ütleb, et süsteem

$$b_1, a_1, a_2, \ldots, a_{m-1} \tag{U_1}$$

on V moodustajate süsteem. Süsteemi U_1 võib vaadelda kui süsteemi, mis on saadud süsteemist A ühe vektori asendamisel süsteemi B esimese vektoriga. Oletame, et me oleme selliseid asendusi tehes jõudnud moodustajate süsteemini

$$b_i, b_{i-1}, \ldots, b_1, a_1, a_2, \ldots, a_{m-i} \tag{U_i}$$

(olles võibolla vajaduse korral A vektoreid ümber nummerdanud), kus $i \in \{1, \ldots, m-1\}$. Siis muuhulgas ka vektor b_{i+1} avaldub süsteemi U_i kaudu, mis tähendab, et süsteem

$$b_{i+1}, b_i, b_{i-1}, \ldots, b_1, a_1, a_2, \ldots, a_{m-i} \tag{T_{i+1}}$$

on lineaarselt sõltuv. Järelikult peab üks selle süsteemi vektoritest avalduma eelnevate lineaarkombinatsioonina. See vektor ei saa kuuluda hulka $b_{i+1}, b_i, b_{i-1}, \ldots, b_1$, sest muidu peaks süsteem B olema lineaarselt sõltuv. Seega peab eelnevate lineaarkombinatsioonina avalduma üks vektoritest $a_1, a_2, \ldots, a_{m-i}$. Vajaduse korral vektoreid ümber nummerdades võime eeldada, et see on vektor a_{m-i}. Järelikult

$$V = L(b_{i+1}, b_i, \ldots, b_1, a_1, a_2, \ldots, a_{m-i}) = L(b_{i+1}, b_i, \ldots, b_1, a_1, a_2, \ldots, a_{m-(i+1)}).$$

Viimane võrdus ütleb, et süsteem

$$b_{i+1}, b_i, \ldots, b_1, a_1, a_2, \ldots, a_{m-(i+1)} \tag{U_{i+1}}$$

on V moodustajate süsteem. Niiviisi jätkates ja vektoreid a_j välja vahetades jõuame m-ndal sammul moodustajate süsteemini

$$b_m, b_{m-1}, \ldots, b_1. \tag{U_m}$$

Siis aga süsteem $B = \{b_1, \ldots, b_m, b_{m+1}, \ldots, b_n\}$ ei ole minimaalne moodustajate süsteem, mis on vastuolus teoreemiga 6.40. Järelikult m ei ole väiksem kui n. Analoogiliselt saab näidata, et n ei ole väiksem kui m ja seega $m = n$. □

Fakt, et baasivektorite arv ei sõltu baasi valikust lubab meil anda järgmise väga olulise definitsiooni.

Definitsioon 6.42 Vektorruumi **mõõtmeks** ehk **dimensiooniks** nimetatakse vektorite arvu selle vektorruumi mingis baasis. Ainult nullvektorist koosneva vektorruumi mõõtmeks loetakse arv 0. Vektorruumi V mõõdet tähistatakse järgmiselt: $\dim(V)$.

Näide 6.43 1. Kui K on korpus ja $n \in \mathbb{N}$, siis vektorruumi K^n mõõde on n, sest üheks baasiks selles vektorruumis on näites 6.34 toodud baas $e_1, \ldots, e_n$.

2. Vektorruumi $\mathrm{Mat}_{m,n}(K)$ mõõde on mn, sest baasivektoreiks võib võtta kõik maatriksid, milles on ühel kohal 1 ja ülejäänud kohtadel 0-d.

Lause 6.44 *n-mõõtmelises vektorruumis on iga n lineaarselt sõltumatust vektorist koosnev süsteem baas.*

Tõestus. Olgu $a_1, \ldots, a_n$ lineaarselt sõltumatu vektorite süsteem n-mõõtmelises vektorruumis V. Lausest 6.37 teame, et iga lineaarselt sõltumatu vektorite süsteemi saab täiendada baasiks. Kuna aga kõigis baasides on n vektorit, siis peabki süsteem $a_1, \ldots, a_n$ olema juba baas. □

6.6 Vektori koordinaadid

Ilmselt on lugeja kooliprogrammist tuttav analüütilise geomeetria algetega, kus kesksel kohal on vektori koordinaatide mõiste. Tuleb välja, et koordinaatidest saab rääkida mitte ainult geomeetrilistes vektorruumides $\mathbb{E}_2$ ja $\mathbb{E}_3$ vaid suvalistes mittetriviaalsetes vektorruumides.

Lause 6.45 *Vektorruumi $V \neq \{0\}$ iga vektor on üheselt avaldatav baasivektorite lineaarkombinatsioonina.*

Tõestus. Olgu V vektorruum üle korpuse K ja olgu $e = \{e_1, e_2, \ldots, e_n\}$ selle vektorruumi baas. Kuna e on moodustajate süsteem, siis saab iga vektori avaldada vektorite $e_1, \ldots, e_n$ lineaarkombinatsioonina. Oletame nüüd, et vektor $a \in V$ on avaldatav kahel viisil:

$$a = a_1e_1 + a_2e_2 + \ldots + a_ne_n = b_1e_1 + b_2e_2 + \ldots + b_ne_n,$$

kus $a_1, \ldots, a_n, b_1, \ldots, b_n \in K$. Siis

$$(a_1 - b_1)e_1 + (a_2 - b_2)e_2 + \ldots + (a_n - b_n)e_n = 0,$$

millest lineaarse sõltumatuse tõttu saame, et $a_1 - b_1 = a_2 - b_2 = \ldots = a_n - b_n = 0$ ehk

$$a_1 = b_1,\ a_2 = b_2,\ \ldots,\ a_n = b_n.$$

□

Tõestatud lause lubab defineerida vektori koordinaadid baasi suhtes.

Definitsioon 6.46 Olgu V vektorruum üle korpuse K, olgu $e = \{e_1, e_2, \ldots, e_n\}$ selle vektorruumi baas ja $a \in V$. Kui $a = a_1e_1 + a_2e_2 + \ldots + a_ne_n$, siis skalaare $a_1, a_2, \ldots, a_n \in K$ nimetatakse vektori a **koordinaatideks** baasi e suhtes.

Lause 6.47 *Olgu V vektorruum üle korpuse K ja olgu $e = \{e_1, e_2, \ldots, e_n\}$ selle vektorruumi baas. Kui vektori a koordinaadid baasi e suhtes on $a_1, \ldots, a_n$ ja vektori b koordinaadid baasi e suhtes on $b_1, \ldots, b_n$, siis vektori $a + b$ koordinaadid baasi e suhtes on $a_1 + b_1, \ldots, a_n + b_n$ ja vektori ka (kus $k \in K$) koordinaadid baasi e suhtes on $ka_1, \ldots, ka_n$.*

Tõestus. Kui $a = a_1e_1 + a_2e_2 + \ldots + a_ne_n$ ja $b = b_1e_1 + b_2e_2 + \ldots + b_ne_n$, siis

$$a + b = (a_1e_1 + \ldots + a_ne_n) + (b_1e_1 + \ldots + b_ne_n) = (a_1 + b_1)e_1 + \ldots + (a_n + b_n)e_n$$

ja

$$ka = k(a_1e_1 + \ldots + a_ne_n) = (ka_1)e_1 + \ldots + (ka_n)e_n.$$

□

7 Astak

Selles päätükis tutvume astaku mõistega ja selle arvutamise meetoditega. Astakust saab rääkida nii maatriksite kui ka suvaliste vektorite süsteemide korral.

7.1 Vektorite süsteemi astak

Definitsioon 7.1 Vektorite süsteemi **astakuks** nimetatakse selle vektorite süsteemi lineaarse katte mõõdet.

Süsteemi $a_1, \ldots, a_s$ astakut tähistatakse sümboliga $\operatorname{rank}(a_1, \ldots, a_s)$. Definitsiooni põhjal

$$\boxed{\operatorname{rank}(a_1, \ldots, a_s) = \dim(L(a_1, \ldots, a_s)).}$$

Lause 7.2 *Vektorite süsteemi astak on võrdne vektorite arvuga selle süsteemi mistahes maksimaalses lineaarselt sõltumatus alamsüsteemis.*

Tõestus. Vaatleme vektorruumi V vektorite süsteemi $a_1, \ldots, a_s$. Olgu selle süsteemi astak r, s.t. $r = \dim(L(a_1, \ldots, a_s))$. Vaatleme süsteemi $a_1, \ldots, a_s$ mingit maksimaalset lineaarselt sõltumatut alamsüsteemi. Vajaduse korral vektoreid ümber nummerdades võime eeldada, et see süsteem koosneb vektoritest $a_1, \ldots, a_t$, kus $t \leqslant s$. Peame näitama, et $t = r$.

Kuna $a_1, \ldots, a_t$ on maksimaalne lineaarselt sõltumatu alamsüsteem, siis lisades süsteemile $a_1, \ldots, a_t$ vektori a_i, kus $i \in \{t+1, \ldots, s\}$, saame lineaarselt sõltuva süsteemi, milles mingi vektor peab avalduma eelnevate lineaarkombinatsioonina. See saab olla vaid a_i. Seega vektorid $a_{t+1}, \ldots, a_s$ avalduvad vektorite $a_1, \ldots, a_t$ kaudu, mis järelduse 6.32 põhjal tähendab, et $L(a_1, \ldots, a_t, a_{t+1}, \ldots, a_s) = L(a_1, \ldots, a_t)$. Seega

$$r = \dim(L(a_1, \ldots, a_s)) = \dim(L(a_1, \ldots, a_t)) = t,$$

sest $a_1, \ldots, a_t$ on $L(a_1, \ldots, a_t)$ lineaarselt sõltumatu moodustajate süsteem ehk baas. □

Näide 7.3 Kui vektorid a, b, c on lineaarselt sõltumatud, siis a, b, c on süsteemi $a, b, b, c, 2a+c, a$ maksimaalne lineaarselt sõltumatu alamsüsteem ja $\operatorname{rank}(a, b, b, c, 2a + c, a) = 3$.

Definitsioon 7.4 Vektorruumi V kahte vektorite süsteemi nimetatakse **ekvivalentseteks**, kui nende süsteemide lineaarsed katted on võrdsed.

Seega süsteemid $a_1, \ldots, a_s$ ja $b_1, \ldots, b_t$ on ekvivalentsed, kui

$$L(a_1, \ldots, a_s) = L(b_1, \ldots, b_t).$$

On lihtne aru saada, et ekvivalentsuse seos vektorruumi V vektorite süsteemide vahel on refleksiivne, sümmeetriline ja transitiivne.

Nii nagu maatriksi ridade puhulgi (vt. definitsiooni 3.6), võib suvalise vektorite süsteemi korral vaadelda järgmisi teisendusi.

Definitsioon 7.5 Vektorite süsteemi **elementaarteisendused** on järgmised teisendused:

1. süsteemi kahe vektori äravahetamine;
2. süsteemi vektori korrutamine nullist erineva skalaariga;

3. süsteemi mingile vektorile mingi skalaariga korrutatud teise vektori liitmine.

Lause 7.6 *Kui vektorruumi V vektorite süsteem T on saadud süsteemist S elementaarteisenduste abil, siis süsteemid S ja T on ekvivalentsed.*

TÕESTUS. Tänu ekvivalentsusseose transitiivsusele piisab, kui vaatleme süsteemi T, mis on saadud süsteemist S ühe elementaarteisenduse abil.

1. On selge, et vektorite järjekorra muutmine ei muuda süsteemi lineaarset katet.

2. Teist tüüpi teisenduste korral jätame tõestuse läbimõtlemiseks lugejale.

3. Näitame, et mistahes skalaari k, vektorite $a_1, \ldots, a_s$ ja indeksite $i, j \in \{1, \ldots, s\}$, $i < j$ korral

$$L(a_1, \ldots, a_i, \ldots, a_j, \ldots, a_s) = L(a_1, \ldots, a_i + ka_j, \ldots, a_j, \ldots, a_s). \tag{28}$$

Kuna mistahes skalaaride $k_1, \ldots, k_s$ ja $l_1, \ldots, l_s$ korral

$$\begin{aligned}
&k_1a_1 + \ldots + k_ia_i + \ldots + k_ja_j + \ldots + k_sa_s \\
&= k_1a_1 + \ldots + k_i(a_i + ka_j) + \ldots + (k_j - kk_i)a_j + \ldots + k_sa_s, \\
&l_1a_1 + \ldots + l_i(a_i + ka_j) + \ldots + l_ja_j + \ldots + l_sa_s \\
&= l_1a_1 + \ldots + l_ia_i + \ldots + (l_ik + l_j)a_j + \ldots + l_sa_s,
\end{aligned}$$

siis võrduse (28) vasakul poolel olev hulk sisaldub paremal poolel olevas hulgas ja vastupidi. □

7.2 Maatriksi astak

Maatriksi korral võib rääkida tema rea- ja veeruvektoritest.

Definitsioon 7.7 Maatriksi $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(K)$ i-ndaks **reavektoriks** nimetatakse vektorit

$$A_i := (a_{i1}, a_{i2}, \ldots, a_{in}) \in K^n$$

ja i-ndaks **veeruvektoriks** nimetatakse vektorit

$$(a_{1i}, a_{2i}, \ldots, a_{mi}) \in K^m.$$

Seega põhimõtteliselt võiks maatriksit $A \in \mathrm{Mat}_{m,n}(K)$ vaadelda kui hulga $(K^n)^m$ elementi kirjutades selle ridade kaupa kujul

$$A = ((a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})) = (A_1, A_2, \ldots, A_n),$$

või kui hulga $(K^m)^n$ elementi, kui kirjutame A veergude kaupa. Esimest viisi maatriksi esitamiseks kasutatakse mitmetes arvutialgebra süsteemides (nt. Maple, Mathematica).

Definitsioon 7.8 Maatriksi astakuks nimetatakse selle maatriksi reavektorite süsteemi astakut. Maatriksi A astakut tähistatakse sümboliga $\mathrm{rank}(A)$.

Formaalselt võib kirjutada, et

$$\mathrm{rank}(A) = \dim(L(A_1, \ldots, A_m)).$$

Tänu lausele 7.2 on maatriksi A astak võrdne lineaarselt sõltumatute reavektorite maksimaalse arvuga. Teiste sõnadega: *maatriksi A astak on r siis ja ainult siis, kui*

1. *sellel maatriksil leidub r lineaarselt sõltumatut reavektorit,*

2. *neile r vektorile mistahes reavektori lisamisel saame lineaarselt sõltuva süsteemi.*

Näide 7.9 Maatriksi

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & -1 & 1 \\ 0 & 2 & 1 & 3 & -1 \\ 2 & 2 & 0 & -2 & 2 \end{pmatrix}$$

astak on 2, sest reavektorid A_2 ja A_3 on lineaarselt sõltumatud, aga süsteemid A_1, A_2, A_3 ja A_2, A_3, A_4 on lineaarselt sõltuvad (Miks?).

Kehtib järgmine oluline teoreem (mille tõestust me käesolevas kursuses ei anna).

Teoreem 7.10 (Teoreem maatriksi astakust) *Maatriksi astak on võrdne selle maatriksi nullist erinevate miinorite kõrgeima järguga.*

Niisiis: *maatriksi astak on r siis ja ainult siis, kui*

1. *selles maatriksis leidub r-ndat järku nullist erinev miinor,*

2. *kõik suuremat järku miinorid on võrdsed nulliga.*

Kuna alamruutmaatriksi B determinant on võrdne maatriksi B^T determinandiga, siis maatriksi A transponeerimisel tema nullist erinevate miinorite kõrgeim järk ei muutu. Seega saame teoreemist 7.10 järgmise järelduse.

Järeldus 7.11 *Maatriksi astak ei muutu transponeerimisel, s.t.*

$$\boxed{\operatorname{rank}(A) = \operatorname{rank}(A^T).}$$

Järeldus 7.12 *Maatriksi astak on võrdne selle maatriksi veeruvektorite süsteemi astakuga.*

Tõestus. Kuna $\operatorname{rank}(A) = \operatorname{rank}(A^T)$, siis $\operatorname{rank}(A)$ on võrdne maatriksi A^T reavektorite süsteemi astakuga. Viimane aga on võrdne maatriksi A veeruvektorite süsteemi astakuga. □

Edasises läheb meil vaja ka järgmist tulemust.

Lause 7.13 *Ruutmaatriksi reavektorid on lineaarselt sõltuvad parajasti siis, kui selle maatriksi determinant on* 0.

Tõestus. Tarvilikkus. Kui maatriksi A reavektorid on lineaarselt sõltuvad, siis leidub nende hulgas mingi reavektor, mis avaldub eelnevate lineaarkombinatsioonina. Olgu näiteks $A_i = k_1A_1 + \ldots + k_{i-1}A_{i-1}$. Liites sellele reale sobiva skalaariga korrutatud eelnevad read saame i-nda rea muuta nullreaks ja seega on $|A| = 0$.
Piisavus. Kui $A \in \operatorname{Mat}_n(K)$ ja $|A| = 0$, siis selles maatriksis ei leidu n-ndat järku nullist erinevat miinorit. Seega teoreemi 7.10 põhjal $\operatorname{rank}(A) < n$, mis tähendab, et maatriksi A reavektorite süsteemi astak on väiksem kui n. Seega reavektorite hulgas ei saa olla n lineaarselt sõltumatut vektorit. Järelikult A reavektorite süsteem on lineaarselt sõltuv. □

7.3 Astaku arvutamisest

Põhiliseks meetodiks maatriksi astaku leidmisel on **elementaarteisenduste meetod**. Selle meetodi puhul tehakse elementaarteisendusi maatriksi ridade ja veergudega, et muuta maatriks "lihtsamaks" (selle lihtsuse all mõeldakse enamasti seda, et maatriksis oleks võimalikult palju nulle). Harilikult on eesmärgiks viia maatriks nn. astmelisele kujule.

Definitsioon 7.14 Öeldakse, et maatriks on **astmelisel kujul**, kui

1. nullidest koosnevad read on nullist erinevaid elemente sisaldavatest ridadest allpool;
2. iga $i \geqslant 2$ korral i-nda rea esimene nullist erinev element (kui see leidub) on kaugemal (s.t. tema veeruindeks on suurem), kui $(i-1)$-se rea esimene nullist erinev element.

Niisiis maatriks on astmelisel kujul, kui tal on kuju

$$\begin{pmatrix}
0 & \dots & 0 & a_{1j_1} & \dots & a_{1,j_2-1} & a_{1j_2} & \dots & a_{1,j_3-1} & a_{1j_3} & \dots & \dots & \dots & \dots & a_{1n} \\
0 & \dots & 0 & 0 & \dots & 0 & a_{2j_2} & \dots & a_{2,j_3-1} & a_{2j_3} & \dots & \dots & \dots & \dots & a_{2n} \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & a_{3j_3} & \dots & \dots & \dots & \dots & a_{3n} \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & a_{rj_r} & \dots & a_{rn} \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0
\end{pmatrix}, \tag{29}$$

kus

$$1 \leqslant j_1 < j_2 < j_3 < \ldots < j_r \leqslant n$$

ja elemendid $a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$ on nullist erinevad. Sellise kuju puhul ütleme, et astmelises kujus on r astet ja et astmekohad on $(1, j_1), (2, j_2), \ldots, (r, j_r)$.

Näide 7.15 Maatriks

$$\begin{pmatrix}
2 & 1 & 3 & 0 \\
0 & 4 & 0 & 1 \\
0 & 0 & 0 & 7 \\
0 & 0 & 0 & 0
\end{pmatrix}$$

on astmelisel kujul, kusjuures astmeid on 3.

Lause 7.16 *Iga maatriksi saab ridade elementaarteisenduste abil viia astmelisele kujule.*

Tõestus. Otsime maatriksis A üles esimese veeru, milles leidub nullist erinevaid elemente. Olgu selle veeru number j_1. Ridade järjekorra vahetamisega võime saavutada olukorra, kus j_1-se veeru esimene element on nullist erinev. Selle elemendi abil saab kolmandat tüüpi teisenduste abil muuta nulliks kõik ülejäänud elemendid j_1-ses veerus. Leiame nüüd järgmise veeru, mis sisaldab nullist erinevaid elemente esimesest reast allpool. Olgu selle veeru number j_2. Ridade vahetamisega võime saavutada, et kohal $(2, j_2)$ on nullist erinev element b. Muudame liitmisteisendusega nulliks kõik elemendid b all. Jätkame samas vaimus kuni jõuame viimase veeruni. □

Lause 7.17 *Maatriksi astak on võrdne astmete arvuga selle maatriksi astmelises kujus.*

TÕESTUS. Kuna lause 7.6 tõttu elementaarteisendused ei muuda maatriksi astakut, siis on maatriksi ja tema astmelise kuju astakud võrdsed. Kui maatriksi astmeline kuju on (29), siis selles maatriksis ridades $1, 2, \ldots, r$ ja veergudes $j_1, j_2, \ldots, j_r$ on nullist erinev r-ndat järku miinor

$$\begin{vmatrix} a_{1j_1} & a_{1j_2} & \ldots & a_{1j_r} \\ 0 & a_{2j_2} & \ldots & a_{2j_r} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_{rj_r} \end{vmatrix} = a_{1j_1}a_{2j_2}\ldots a_{rj_r}.$$

Samas kõik suuremat järku miinorid on võrdsed nulliga, sest nad sisaldavad vähemalt ühe nullidest koosneva rea. Teoreemi 7.10 tõttu on antud maatriksi astak r, mis ühtlasi on võrdne astmete arvuga astmelises kujus. □

Teine võimalus maatriksi astaku arvutamiseks on kasutada niinimetatud **miinorite ääristamise meetodit**. Öeldakse, et maatriksi A miinor M' **ääristab** maatriksi A miinorit M, kui M' on saadud miinorist M ühe rea ja ühe veeru lisamisel. Meetod põhineb järgmisel faktil (mida me siinkohal ei tõesta).

Lause 7.18 *Kui M on maatriksi A r-ndat järku nullist erinev miinor ja kõik miinorit M ääristavad miinorid on võrdsed nulliga, siis* $\operatorname{rank}(A) = r$.

8 Lineaarvõrrandisüsteemid

Selles peatükis uurime lineaarvõrrandisüsteemide lahendamist. Otsime vastust järgmistele küsimustele.

- Millal on lineaarvõrrandisüsteem lahenduv?
- Kui palju on lineaarvõrrandisüsteemil lahendeid?
- Kuidas neid lahendeid leida?

Üldiste lineaarvõrrandisüsteemide kõrval uurime ka teatud erikujulisi süsteeme, näiteks homogeenseid süsteeme.

8.1 Ülesande püstitus

Definitsioon 8.1 Lineaarvõrrandisüsteem üle korpuse K on võrrandisüsteem kujul

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\qquad\qquad\quad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m, \end{cases} \tag{30}$$

kus $x_1, \ldots, x_n$ on tundmatud ja $a_{11}, \ldots, a_{mn}, b_1, \ldots, b_m \in K$. Elemente $a_{11}, \ldots, a_{mn} \in K$ nimetatakse selle **võrrandisüsteemi kordajateks** ja elemente $b_1, \ldots, b_m \in K$ nimetatakse **vabaliikmeteks**. Märgime, et nii võrrandite arv m, kui tundmatute arv n võivad olla suvalised naturaalarvud.

Definitsioon 8.2 Võrrandisüsteemi (30) **lahendiks** (ehk **erilahendiks**) nimetatakse hulga K^n iga elementi $(k_1, \ldots, k_n)$, mille korral

$$a_{i1}k_1 + a_{i2}k_2 + \ldots + a_{in}k_n = b_i,$$

kus $i = 1, \ldots, m$.

Seega $(k_1, \ldots, k_n)$ on süsteemi (30) lahend, kui iga i korral asendades $k_1, \ldots, k_n$ süsteemi i-ndas võrrandis tundmatute $x_1, \ldots, x_n$ asemele ja arvutades välja vastava K elemendi saame tulemuseks b_i.

Lineaarvõrrandisüsteemi **lahendamise** all peetakse silmas selle süsteemi kõigi lahendite leidmist.

Märkus 8.3 Lineaarvõrrandisüsteemide lahendamisel ei paku meile huvi sellised süsteemid, kus mingi tundmatu x_i kordaja kõigis võrrandites on null. Tõepoolest, kui me oskaksime lahendada süsteeme, kus selliseid tundmatuid ei ole, siis oskaksime vajaduse korral lahendada ka süsteeme, kus selliseid tundmatuid on. Näiteks vaatleme süsteemi, mis koosneb ainult ühest võrrandist $x + y + 0 \cdot z = 0$. Leiame kahe tundmatuga süsteemi $x + y = 0$ kõik lahendid. Nendeks on paarid $(k, -k)$, kus $k \in K$. Siis süsteemi $x + y + 0 \cdot z = 0$ lahenditeks on kõik kolmikud $(k, -k, l)$, kus $k, l \in K$.

Seega *eeldame edaspidises, et kõigis vaadeldavates süsteemides on iga tundmatu vähemalt ühes võrrandis nullist erineva kordajaga.*

Definitsioon 8.4 Lineaarvõrrandisüsteemi nimetatakse

- **mittelahenduvaks** ehk **vasturääkivaks**, kui tal ei ole ühtegi lahendit,
- **lahenduvaks** ehk **kooskõlaliseks**, kui tal on vähemalt üks lahend,
- **üheselt lahenduvaks** ehk **määratuks**, kui tal on täpselt üks lahend.

Definitsioon 8.5 Maatriksit

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

nimetatakse **lineaarvõrrandisüsteemi** (30) **maatriksiks**. Maatriksit

$$A' = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

nimetatakse **lineaarvõrrandisüsteemi** (30) **laiendatud maatriksiks**. Üheveerulist maatriksit

$$\overline{x} = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$$

nimetatakse **lineaarvõrrandisüsteemi** (30) **tundmatute veeruks** ja üheveerulist maatriksit

$$\overline{b} = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix}$$

nimetatakse **lineaarvõrrandisüsteemi** (30) **vabaliikmete veeruks**.

Kuna süsteemi (30) kõigi lahendite $k = (k_1, \dots, k_n) \in K^n$ leidmine on samaväärne kõigi selliste maatriksite

$$\overline{k} = \begin{pmatrix} k_1 \\ k_2 \\ \dots \\ k_n \end{pmatrix} \in \mathrm{Mat}_{n,1}(K)$$

leidmisega, mille korral

$$A\overline{k} = \overline{b},$$

siis räägitakse ka süsteemi (30) **maatrikskujust**

$$A\overline{x} = \overline{b}.$$

8.2 Gaussi meetod

Selles paragrahvis anname meetodi suvalise lineaarvõrrandisüsteemi lahendamiseks.

Definitsioon 8.6 Kahte n tundmatuga lineaarvõrrandisüsteemi üle korpuse K nimetatakse **ekvivalentseteks**, kui neil on ühed ja samad lahendid.

On selge, et lineaarvõrrandisüsteemide ekvivalentsuse seos on refleksiivne, sümmeetriline ja transitiivne.

Lause 8.7 *Kui lineaarvõrrandisüsteemi laiendatud maatriksi reavektorite süsteemiga teha elementaarteisendusi või jätta sellest välja nullvektorid, siis tulemuseks saadavale maatriksile vastav lineaarvõrrandisüsteem on ekvivalentne esialgsega.*

Tõestus. Meenutame (vt. definitsiooni 3.6), et elementaarteisendusi maatriksi ridadega on kolme tüüpi ja nende tegemine on samaväärne maatriksi korrutamisega vasakult elementaarmaatriksitega (lause 3.9). Seega peame näitama, et kui lineaarvõrrandisüsteemi laiendatud maatriks on $A' \in \mathrm{Mat}_{m,n+1}(K)$ ja me korrutame selle vasakult elementaarmaatriksiga C, siis maatriksitele A' ja CA' vastavad lineaarvõrrandisüsteemid on ekvivalentsed. Kui esialgse lineaarvõrrandisüsteemi maatriks on A ja vabaliikmete veerg $\overline{b}$, siis selle süsteemi maatrikskuju on

$$A\overline{x} = \overline{b}. \tag{31}$$

Pärast elementaarteisendust saadava süsteemi maatrikskuju on

$$(CA)\overline{x} = C\overline{b}. \tag{32}$$

Kui nüüd $\overline{k} \in \mathrm{Mat}_{n,1}(K)$ on süsteemi (31) lahend, siis $A\overline{k} = \overline{b}$. Korrutades selle võrduse mõlemad pooled maatriksiga C saame $CA\overline{k} = C\overline{b}$, mis tähendab, et $\overline{k}$ on ka süsteemi (32) lahend. Vastupidi, kui $\overline{k} \in \mathrm{Mat}_{n,1}(K)$ on süsteemi (32) lahend, siis $CA\overline{k} = C\overline{b}$. Kuna kõik elementaarmaatriksid on pööratavad, siis võime viimase võrduse pooli korrutada vasakult maatriksiga C^{-1}. See annab meile võrduse $A\overline{k} = \overline{b}$, kust näeme, et $\overline{k}$ on süsteemi (31) lahend. Seega on neil kahel süsteemil täpselt samad lahendid.

On ka selge, et kui süsteemist jätta välja võrrand $0 \cdot x_1 + \ldots + 0 \cdot x_n = 0$ (ehk laiendatud maatriksist jätta välja nullidest koosnev rida), siis saadaval süsteemil on samad lahendid, mis esialgsel. □

Tõestatud lause lubab lineaarvõrrandisüsteemi lihtsustada nii, et lahendite hulk selle käigus ei muutu. Just tänu sellele lausele võib öelda, et paragrahvis 1.1 vaadeldud lineaarvõrrandisüsteemil on täpselt üks lahend $(-1, 3)$.

Järgnevalt leiame tarviliku ja piisava tingimuse selleks, et lineaarvõrrandisüsteem oleks lahenduv. Osutub, et selle üle saab otsustada astakute põhjal.

Teoreem 8.8 (Kroneckeri-Capelli teoreem)[4] *Lineaarvõrrandisüsteem on lahenduv parajasti siis, kui selle süsteemi maatriksi astak on võrdne selle süsteemi laiendatud maatriksi astakuga.*

Tõestus. Vaatleme lineaarvõrrandisüsteemi, mille maatriks on A ja laiendatud maatriks on A'. Teeme maatriksi A' ridadega selliseid elementaarteisendusi, mis viivad maatriksi A astmelisele kujule. See on võimalik tänu lausele 7.16. Tulemuseks on maatriks kujul

[4] Leopold Kronecker (1823–1891) — saksa matemaatik,
Alfredo Capelli (1855–1910) — itaalia matemaatik.

$$\begin{pmatrix} a_{11} & \dots & a_{1,j_2-1} & a_{1j_2} & \dots & a_{1,j_{3-1}} & a_{1j_3} & \dots & \dots & \dots & \dots & a_{1n} & b_1 \\ 0 & \dots & 0 & a_{2j_2} & \dots & a_{2,j_{3-1}} & a_{2j_3} & \dots & \dots & \dots & \dots & a_{2n} & b_2 \\ 0 & \dots & 0 & 0 & \dots & 0 & a_{3j_3} & \dots & \dots & \dots & \dots & a_{3n} & b_3 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & a_{rj_r} & \dots & a_{rn} & b_r \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_{r+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_m \end{pmatrix}, \tag{33}$$

kus

$$1 < j_2 < j_3 < \ldots < j_r \leqslant n$$

ja elemendid $a_{11}, a_{2j_2}, \ldots, a_{rj_r}$ on nullist erinevad. Juhime tähelepanu, et siin $a_{11} \neq 0$ tänu meie kokkuleppele, et x_1 kordaja mingis võrrandis peab olema nullist erinev. Lause 8.7 põhjal on esialgne lineaarvõrrandisüsteem ekvivalentne maatriksile (33) vastava lineaarvõrrandisüsteemiga. Muuhulgas on nad samaaegselt kas lahenduvad või mittelahenduvad. Seega piisab kui vaatleme maatriksile (33) vastava süsteemi lahenduvust.

Astmete arvu järgi näeme, et süsteemi maatriksi astak on r (vt. lauset 7.17). Oletame, et laiendatud maatriksi astak ei võrdu süsteemi maatriksi astakuga r. Siis laiendatud maatriksi astak peab olema suurem kui r, s.t. mõni elementidest $b_{r+1}, \ldots, b_m$ peab olema nullist erinev. Siis on meil süsteemis võrrand $0 \cdot x_1 + \ldots + 0 \cdot x_n = b_i$, kus $b_i \neq 0$. Sellisel võrrandil ei ole ühtegi lahendit ja seega süsteem ei ole lahenduv. Järelikult kui süsteem on lahenduv, siis $b_{r+1} = \ldots = b_m = 0$ ja süsteemi maatriksi astak on võrdne selle süsteemi laiendatud maatriksi astakuga.

Tõestame nüüd vastupidise implikatsiooni. Olgu süsteemi maatriksi astak võrdne selle süsteemi laiendatud maatriksi astakuga, s.t. $b_{r+1} = \ldots = b_m = 0$. Näitame, et sellel süsteemil leidub lahend $(k_1, \ldots, k_n) \in K^n$, kus $k_i = 0$ iga $i \in \{1, \ldots, n\} \setminus \{1, j_2, \ldots, j_r\}$ korral. Sellise lahendi saame leida, kui oskame ära lahendada süsteemi

$$\begin{cases} a_{11}x_1 + a_{1j_2}x_{j_2} + \ldots + \quad a_{1j_{r-1}}x_{j_{r-1}} + \quad a_{1j_r}x_{j_r} = b_1 \\ \qquad\quad a_{2j_2}x_{j_2} + \ldots + \quad a_{2j_{r-1}}x_{j_{r-1}} + \quad a_{2j_r}x_{j_r} = b_2 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots \\ \qquad\qquad\qquad\qquad\quad a_{r-1,j_{r-1}}x_{j_{r-1}} + a_{r-1,j_r}x_{j_r} = b_{r-1}. \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad a_{rj_r}x_{j_r} = b_r. \end{cases}$$

Viimane süsteem on aga tõesti lahenduv. Viimasest võrrandist arvutame $x_{j_r} = a_{rj_r}^{-1} b_r$. Siis asendame saadud väärtuse eelviimasesse võrrandisse ja arvutame välja $x_{j_{r-1}}$ väärtuse jne. □

Näitame nüüd kuidas saab leida lahenduva süsteemi lahendeid. Oletame, et meil on tegemist lahenduva süsteemiga, mille laiendatud maatriks on viidud astmelisele kujule (33), kus $b_{r+1} = \ldots = b_m = 0$. Jätame sellest maatriksist välja nullidest koosnevad read. Lause 8.7 tõttu ei muuda see võrrandisüsteemi lahendite hulka. Niisiis vaatleme lineaarvõrrandisüsteemi laiendatud maatriksiga

$$\begin{pmatrix} a_{11} & \dots & a_{1,j_2-1} & a_{1j_2} & \dots & a_{1,j_{3-1}} & a_{1j_3} & \dots & \dots & \dots & \dots & a_{1n} & b_1 \\ 0 & \dots & 0 & a_{2j_2} & \dots & a_{2,j_{3-1}} & a_{2j_3} & \dots & \dots & \dots & \dots & a_{2n} & b_2 \\ 0 & \dots & 0 & 0 & \dots & 0 & a_{3j_3} & \dots & \dots & \dots & \dots & a_{3n} & b_3 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & a_{rj_r} & \dots & a_{rn} & b_r \end{pmatrix}, \tag{34}$$

On kaks võimalust.

1) $r = n$. See tähendab, et $j_2 = 2$, $j_3 = 3$, ..., $j_n = n$ ning maatriksile (34) vastav süsteem on kujul

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1,n-1}x_{n-1} + a_{1n}x_n = b_1 \\ a_{22}x_2 + \ldots + a_{2,n-1}x_{n-1} + a_{2n}x_n = b_2 \\ \ldots \\ + a_{n-1,n-1}x_{n-1} + a_{n-1,n}x_n = b_{n-1}. \\ a_{nn}x_n = b_n. \end{cases}$$

Viimasest võrrandist näeme, et $x_n = a_{nn}^{-1}b_n$. Asendades selle eelviimasesse võrrandisse saame välja arvutada x_{n-1} väärtuse jne. Niisiis sellisel juhul on süsteemil täpselt üks lahend ehk *süsteem on üheselt lahenduv.*

2) $r < n$. Osutub, et sellisel juhul on süsteemil rohkem kui üks lahend (lõpmatu K korral on neid lõpmata palju). Niisuguses olukorras kõigi lahendite esitamiseks jagatakse süsteemi tundmatud kahte rühma: vabadeks ja sõltuvateks tundmatuteks. Nimelt tundmatuid $x_1, x_{j_2}, \ldots, x_{j_r}$ (need on tundmatud, mis vastavad n.ö. astmekohtadele maatriksis (34)) nimetatakse **sõltuvateks tundmatuteks** ja kõiki ülejäänud tundmatuid **vabadeks tundmatuteks**. Paneme tähele, et *sõltuvate tundmatute arv r on võrdne lineaarvõrrandisüsteemi maatriksi astakuga ja vabade tundmatute arv on $n-r$, s.t. kõigi tundmatute arvu ja lineaarvõrrandisüsteemi maatriksi astaku vahe.*

Kuna x_{j_i} ($i \in \{2, \ldots, r\}$) kordaja a_{ij_i} on nullist erinev, siis liites sobiva skalaariga korrutatud i-ndat rida eelnevatele ridadele on j_i-ndas veerus võimalik kõik ülejäänud elemendid nulliks muuta. Viies seejärel vabade tundmatutega liikmed paremale poole võrdusmärki ja korrutades iga võrrandi mõlemaid pooli sobiva skalaariga saame sõltuvad tundmatud avaldada vabade tundmatute ja vabaliikmete kaudu:

$$\begin{cases} x_1 = c_1 + d_{1,r+1}x_{j_{r+1}} + \ldots + d_{1n}x_{j_n} \\ x_{j_2} = c_2 + d_{2,r+1}x_{j_{r+1}} + \ldots + d_{2n}x_{j_n} \\ \quad \ldots \\ x_{j_r} = c_r + d_{r,r+1}x_{j_{r+1}} + \ldots + d_{rn}x_{j_n}, \end{cases} \tag{35}$$

kus $c_1, \ldots, c_r$ on vabaliikmed ja $\{j_{r+1}, \ldots, j_n\} = \{1, 2, \ldots, n\} \setminus \{1, j_2, \ldots, j_r\}$, s.t. $x_{j_{r+1}}, \ldots, x_{j_n}$ on vabad tundmatud. Kui anda nüüd vabadele tundmatutele (n.ö. vabalt) mistahes väärtused $k_{r+1}, \ldots, k_n \in K$ siis saame seoste (35) abil välja arvutada sõltuvate tundmatute $x_1, x_{j_2}, \ldots, x_{j_r}$ väärtused ja seega saame kätte ühe vaadeldava süsteemi lahendi. Teisest küljest on selge, et sellisel viisil saame me kätte kõik vaadeldava süsteemi lahendid, sest kõik lahendid peavad rahuldama seoseid (35). Kui lineaarvõrrandisüsteemi lahendid on antud seoste (35) abil, siis öeldakse, et tegemist on selle süsteemi **üldlahendiga vabade tundmatute kaudu**. Kirjeldatud meetodit lineaarvõrrandisüsteemi lahendamiseks kutsutakse **Gaussi**[5] **meetodiks**.

Märkus 8.9 Maatriksit võib astmelisele kujule viia mitmel erineval viisil ja sellest tulenevalt võib ka saada mitmeid erinevaid sõltuvate (ja vabade) tundmatute komplekte. Kui lahenduva lineaarvõrrandisüsteemi maatriksi astak on r ja meil on selles maatriksi mingid r lineaarselt sõltumatut rida (sellised tingimata leiduvad), siis valides nendes ridades mingi r-ndat järku nullist erineva miinori saame selle miinori teisendada diagonaalkujule ja seega tundmatud, mille kordajate veergudest see miinor on moodustatud, võib võtta sõltuvateks tundmatuteks, sest neid on võimalik ülejäänud tundmatute kaudu avaldada.

[5]Carl Friedrich Gauss (1777–1855) — saksa matemaatik.

Näide 8.10 Lahendame lineaarvõrrandisüsteemi

$$\begin{cases} 2x_1 - 3x_2 + 5x_3 + 7x_4 = 1 \\ 4x_1 - 6x_2 + 2x_3 + 3x_4 = 2 \\ 2x_1 - 3x_2 - 11x_3 - 15x_4 = 1 \end{cases} \tag{36}$$

(üle $\mathbb{R}$) Gaussi meetodil.

Moodustame võrrandisüsteemi laiendatud maatriksi ja teisendame selle astmelisele kujule jättes ära nullidest koosnevad read:

$$\left(\begin{array}{cccc|c} 2 & -3 & 5 & 7 & 1 \\ 4 & -6 & 2 & 3 & 2 \\ 2 & -3 & -11 & -15 & 1 \end{array}\right)\begin{matrix} \\ -2\mathrm{I} \\ -\mathrm{I} \end{matrix} \to \left(\begin{array}{cccc|c} 2 & -3 & 5 & 7 & 1 \\ 0 & 0 & -8 & -11 & 0 \\ 0 & 0 & -16 & -22 & 0 \end{array}\right)\begin{matrix} \\ \\ -2\mathrm{II} \end{matrix} \to$$

$$\left(\begin{array}{cccc|c} 2 & -3 & 5 & 7 & 1 \\ 0 & 0 & -8 & -11 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)\cdot\left(-\tfrac{1}{8}\right) \to \left(\begin{array}{cccc|c} 2 & -3 & 5 & 7 & 1 \\ 0 & 0 & 1 & \frac{11}{8} & 0 \end{array}\right)-5\mathrm{II} \to$$

$$\left(\begin{array}{cccc|c} 2 & -3 & 0 & \frac{1}{8} & 1 \\ 0 & 0 & 1 & \frac{11}{8} & 0 \end{array}\right).$$

Näeme, et nii süsteemi maatriksi kui ka laiendatud maatriksi astak on 2 ja seega süsteem on lahenduv. Sõltuvaid tundmatuid on 2 (sest astak on 2) ja vabu tundmatuid on $4 - 2 = 2$. Astmekohtade järgi võime sõltuvateks tundmatuteks valida x_1 ja x_3, seega vabadeks tundmatuteks jäävad x_2 ja x_4. Avaldades viimast maatriksit kasutades sõltuvad tundmatud vabade kaudu, saame üldlahendi vabade tundmatute kaudu:

$$\begin{cases} x_1 = \frac{1}{2} + \frac{3}{2}x_2 - \frac{1}{16}x_4 \\ x_3 = -\frac{11}{8}x_4 \end{cases}.$$

Seda tuleb tõlgendada nii, et andes vabadele tundmatutele x_2 ja x_4 kõikvõimalikud reaalarvulised väärtused saame välja arvutada vastavad x_1 ja x_3 väärtused ja niimoodi kätte kõik esialgse süsteemi lahendid. See tähendab, et süsteemi kõigi lahendite hulk on

$$L = \left\{ \left(\frac{1}{2} + \frac{3}{2}k - \frac{1}{16}l, k, -\frac{11}{8}l, l \right) \middle| \, k, l \in \mathbb{R} \right\} \subseteq \mathbb{R}^4.$$

Näiteks võttes $k = l = 0$ saame süsteemi (36) üheks erilahendiks $d_* = (\frac{1}{2}, 0, 0, 0)$.

8.3 Crameri peajuht

Vaatleme nüüd lineaarvõrrandisüsteemide lahendamist ühel tähtsal erijuhul.

Definitsioon 8.11 Öeldakse, et lineaarvõrrandisüsteemi puhul on tegemist **Crameri**[6] **peajuhuga**, kui

1. võrrandite arv on võrdne tundmatute arvuga ja
2. süsteemi maatriks on regulaarne.

[6] Gabriel Cramer (1704–1752) — šveitsi matemaatik.

Seega Crameri peajuhuga on tegemist siis, kui lineaarvõrrandisüsteem on kujul

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\qquad\qquad\qquad \ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n, \end{cases} \tag{37}$$

kus $A = (a_{ij}) \in \mathrm{Mat}_n(K)$ on regulaarne (s.t. $|A| \neq 0$).

Lause 8.12 *Kui lineaarvõrrandisüsteemi puhul on tegemist Crameri peajuhuga, siis on sellel süsteemil täpselt üks lahend.*

Tõestus. Meenutame, et vektor $k = (k_1, \ldots, k_n) \in K^n$ on süsteemi (37) lahend parajasti siis, kui üheveeruline maatriks

$$\overline{k} = \begin{pmatrix} k_1 \\ \cdots \\ k_n \end{pmatrix} \in \mathrm{Mat}_{n,1}(K)$$

rahuldab võrdust

$$A\overline{k} = \overline{b}.$$

Et A on regulaarne, siis leidub pöördmaatriks A^{-1}. Järelikult

$$A(A^{-1}\overline{b}) = (AA^{-1})\overline{b} = E\overline{b} = \overline{b},$$

mis tähendab, et süsteemil leidub vähemalt üks lahend (selle komponentideks on üheveerulise maatriksi $A^{-1}\overline{b}$ elemendid). Teisest küljest, kui $k, l \in K^n$ on süsteemi lahendid, siis $A\overline{k} = \overline{b} = A\overline{l}$. Korrutades võrduse $A\overline{k} = A\overline{l}$ mõlemaid pooli vasakult maatriksiga A^{-1} saame võrduse $\overline{k} = \overline{l}$, millest järeldub, et $k = l$. Seega süsteemil on ülimalt üks lahend ja kokkuvõttes peab tal olema täpselt üks lahend. □

Tuleb välja, et Crameri peajuhu korral saab süsteemi lahendi leida determinantide abil.

Nagu nägime lause 8.12 tõestuses peab süsteemi (37) lahendi $k = (k_1, \ldots, k_n) \in K^n$ korral kehtima võrdus

$$\begin{pmatrix} k_1 \\ \cdots \\ k_n \end{pmatrix} = A^{-1}\overline{b}.$$

Teoreemi 3.16 põhjal $A^{-1} = |A|^{-1}(A_{ji})$ (see on maatriks, mille i-ndas reas ja j-ndas veerus on element $|A|^{-1}A_{ji}$, kus A_{ji} on maatriksi A elemendi a_{ji} algebraline täiend). Vastavalt maatriksite korrutamise ja maatriksite võrduse definitsioonile võime kirjutada, et

$$k_i = \sum_{j=1}^{n} \left(|A|^{-1}A_{ji}\right) b_j = |A|^{-1} \cdot \sum_{j=1}^{n} A_{ji}b_j$$

iga $i \in \{1, \ldots, n\}$ korral. Olgu $D = |A|$ ja olgu D_i ($i \in \{1, \ldots, n\}$) sellise maatriksi determinant, mis on saadud maatriksist A selle i-nda veeru asendamisel süsteemi (37) vabaliikmete veeruga, s.t.

$$D_i = \begin{vmatrix} a_{11} & \ldots & a_{1,i-1} & b_1 & a_{1,i+1} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2,i-1} & b_2 & a_{2,i+1} & \ldots & a_{2n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & \ldots & a_{n,i-1} & b_n & a_{n,i+1} & \ldots & a_{nn} \end{vmatrix}$$

Arendades determinanti D_i i-nda veeru järgi saame summa $\sum_{j=1}^{n} A_{ji}b_j$. Järelikult

$$k_i = D^{-1}D_i$$

iga $i \in \{1, \ldots, n\}$ korral. Sellega oleme tõestanud järgmise tulemuse.

Teoreem 8.13 *Kui lineaarvõrrandisüsteemi (37) puhul on tegemist Crameri peajuhuga, siis selle süsteemi lahendi $k = (k_1, \ldots, k_n) \in K^n$ i-s komponent $k_i = D^{-1}D_i$, kus D on selle süsteemi maatriksi determinant ja D_i on sellise maatriksi determinant, mis on saadud süsteemi maatriksist selle i-nda veeru asendamisel süsteemi vabaliikmete veeruga.*

Märkus 8.14 Kui on tegemist Crameri peajuhuga, siis $D \neq 0$ ja arvestades märkust 4.19 võib lahendi leidmise valemid esitada kujul

$$\boxed{k_i = \frac{D_i}{D}, \quad i = 1, \ldots, n.}$$

Neid valemeid kutsutakse **Crameri valemiteks**.

8.4 Homogeennne lineaarvõrrandisüsteem

Definitsioon 8.15 Lineaarvõrrandisüsteemi nimetatakse **homogeenseks**, kui selle süsteemi kõik vabaliikmed on nullid.

Niisiis homogeensel lineaarvõrrandisüsteemil on kuju

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0. \end{cases} \tag{38}$$

Maatrikskujul võib homogeense lineaarvõrrandisüsteemi esitada järgmiselt:

$$A\overline{x} = \overline{0},$$

kus

$$\overline{0} = \begin{pmatrix} 0 \\ \cdots \\ 0 \end{pmatrix} \in \mathrm{Mat}_{m,1}(K).$$

On selge, et nullvektor $(0, \ldots, 0) \in K^n$ on alati homogeense lineaarvõrrandisüsteemi lahend, seega kõik homogeensed lineaarvõrrandisüsteemid on lahenduvad.

Kui mittehomogeense lineaarvõrrandisüsteemi kõigi lahendite hulk on lihtsalt hulga K^n alamhulk, siis homogeensete süsteemide korral võib öelda enamat.

Lause 8.16 *n tundmatuga homogeense lineaarvõrrandisüsteemi (üle korpuse K) kõigi lahendite hulk on alamruum vektorruumis K^n.*

Tõestus. Olgu

$$L = \{k \in K^n \mid A\overline{k} = \overline{0}\}$$

süsteemi (38) kõigi lahendite hulk. Nagu mainitud, see hulk ei ole tühi. Olgu $k, l \in L$ ja $c \in K$. Siis $A(\overline{k+l}) = A(\overline{k} + \overline{l}) = A\overline{k} + A\overline{l} = \overline{0} + \overline{0} = \overline{0}$ ja $A(c\overline{k}) = c(A\overline{k}) = c\overline{0} = \overline{0}$, mis tähendab, et ka $k + l, ck \in L$. □

Vektorruumi alamruum on ise ka vektorruum (vt. lauset 6.9). See lubab anda järgmise definitsiooni.

Definitsioon 8.17 Homogeense lineaarvõrrandisüsteemi lahendite fundamentaalsüsteemiks nimetatakse selle süsteemi lahendite alamruumi baasi.

Teoreem 8.18 *Kui homogeenses lineaarvõrrandisüsteemis on n tundmatut ja selle süsteemi maatriksi astak on r, siis selle süsteemi lahendite fundamentaalsüsteemis on $n-r$ lahendit.*

TÕESTUS. Vaatleme homogeenset lineaarvõrrandisüsteemi kujul (38). Kuna süsteemi maatriksi $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(K)$ astak on r, siis viies maatriksi astmelisele kujule saame maatriksi, kus astmeid on r tükki ning seega ülejäänud read on nullread, millele vastavad võrrandid võib süsteemist välja jätta. Niisiis võime süsteemi maatriksi viia kujule

$$\begin{pmatrix} a'_{11} & \dots & a'_{1,j_2-1} & a'_{1j_2} & \dots & a'_{1,j_3-1} & a'_{1j_3} & \dots & \dots & \dots & \dots & a'_{1n} \\ 0 & \dots & 0 & a'_{2j_2} & \dots & a'_{2,j_3-1} & a'_{2j_3} & \dots & \dots & \dots & \dots & a'_{2n} \\ 0 & \dots & 0 & 0 & \dots & 0 & a'_{3j_3} & \dots & \dots & \dots & \dots & a'_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & a'_{rj_r} & \dots & a'_{rn} \end{pmatrix}, \tag{39}$$

kus

$$1 < j_2 < j_3 < \ldots < j_r \leqslant n$$

ja elemendid $a'_{11}, a'_{2j_2}, \ldots, a'_{rj_r}$ on nullist erinevad. Märgime, et homogeense süsteemi lahendamisel ei ole vaja kasutada vabaliikmete veergu, sest ridade mistahes elementaarteisenduse korral ei teki vabaliikmeks nullist erinevat elementi.

Kui $n = r$, siis $j_2 = 2$, $j_3 = 3$, ..., $j_r = n$, maatriksi (39) determinant on $a'_{11}a'_{22}\ldots a'_{nn} \neq 0$ ja vaadeldava süsteemi puhul on tegemist Crameri peajuhuga. See tähendab, et süsteem on üheselt lahenduv ja lahendite fundamentaalsüsteemis on $0 = n - n$ lahendit.

Kui $r < n$, siis nii nagu ikka Gaussi meetodi korral võtame tundmatud $x_1, x_{j_2}, \ldots, x_{j_r}$ sõltuvateks tundmatuteks ja jätame kõik ülejäänud tundmatud vabadeks tundmatuteks. Vabade tundmatute arv on $n - r$. Sõltuvad tundmatud saame avaldada vabade tundmatute kaudu:

$$\begin{cases} x_1 &= d_{1,r+1}x_{j_{r+1}} + \ldots + d_{1n}x_{j_n} \\ x_{j_2} &= d_{2,r+1}x_{j_{r+1}} + \ldots + d_{2n}x_{j_n} \\ & \dots \\ x_{j_r} &= d_{r,r+1}x_{j_{r+1}} + \ldots + d_{rn}x_{j_n}, \end{cases} \tag{40}$$

kus $\{j_{r+1}, \ldots, j_n\} = \{1, 2, \ldots, n\} \setminus \{1, j_2, \ldots, j_r\}$, s.t. $x_{j_{r+1}}, \ldots, x_{j_n}$ on vabad tundmatud.

Vaatleme nüüd mistahes regulaarset maatriksit

$$\begin{pmatrix} k_{1,j_{r+1}} & k_{1,j_{r+2}} & \dots & k_{1,j_n} \\ k_{2,j_{r+1}} & k_{2,j_{r+2}} & \dots & k_{2,j_n} \\ \dots & \dots & \dots & \dots \\ k_{n-r,j_{r+1}} & k_{n-r,j_{r+2}} & \dots & k_{n-r,j_n} \end{pmatrix} \in \mathrm{Mat}_{n-r}(K),$$

mille järk $n - r$ on võrdne vabade tundmatute arvuga. (Harilikult võetakse selleks maatriksiks ühikmaatriks või mingi diagonaalmaatriks.) Tähistame selle maatriksi reavektorid

$$\begin{aligned} k'_1 &= (k_{1,j_{r+1}}, k_{1,j_{r+2}}, \ldots, k_{1,j_n}), \\ k'_2 &= (k_{2,j_{r+1}}, k_{2,j_{r+2}}, \ldots, k_{2,j_n}), \\ &\dots \\ k'_{n-r} &= (k_{n-r,j_{r+1}}, k_{n-r,j_{r+2}}, \ldots, k_{n-r,j_n}). \end{aligned}$$

Tänu lausele 7.13 on vektorid $k'_1, k'_2, \ldots, k'_{n-r} \in K^{n-r}$ lineaarselt sõltumatud. Anname nüüd iga $i \in \{1, \ldots, n-r\}$ korral vabadele tundmatutele väärtused vaadeldava maatriksi i-ndast reast ja arvutame seoste (40) abil välja sõltuvate tundmatute väärtused. Nii saame $n-r$ süsteemi (38) lahendivektorit $k_1, k_2, \ldots, k_{n-r} \in K^n$. Kui need vektorid oleksid lineaarselt sõltuvad, siis ka vektorid $k'_1, k'_2, \ldots, k'_{n-r}$ peaksid olema lineaarselt sõltuvad. Kuna viimased seda ei ole, siis järelikult on $k_1, k_2, \ldots, k_{n-r}$ lineaarselt sõltumatud.

Tõestuse lõpetamiseks näitame, et vektorite süsteem $k_1, k_2, \ldots, k_{n-r}$ on süsteemi (38) lahendite alamruumi moodustajate süsteem. Selleks peame näitama, et mistahes lahendivektor avaldub nende vektorite lineaarkombinatsioonina. Olgugi $l = (l_1, \ldots, l_n) \in K^n$ süsteemi (38) mingi lahend. Tähistame

$$l' := (l_{j_{r+1}}, \ldots, l_{j_n}) \in K^{n-r}.$$

Siis vektorite süsteem

$$k'_1, k'_2, \ldots, k'_{n-r}, l'$$

on lineaarselt sõltuv, sest tegemist on $n-r+1$ vektoriga $(n-r)$-mõõtmelises vektorruumis. Järelikult peab lause 6.27 põhjal selle süsteemi mingi vektor avalduma eelnevate vektorite lineaarkombinatsioonina. See saab olla ainult vektor l'. Seega leiduvad sellised $u_1, u_2, \ldots, u_{n-r} \in K$, et

$$l' = u_1 k'_1 + u_2 k'_2 + \ldots + u_{n-r} k'_{n-r}. \tag{41}$$

Vaatleme vektorit

$$m := l - u_1 k_1 - u_2 k_2 - \ldots - u_{n-r} k_{n-r}$$

Kuna $l, k_1, k_2, \ldots, k_{n-r}$ on süsteemi (38) lahendid ja selle süsteemi lahendid moodustavad alamruumi vektorruumis K^n, siis ka m on selle süsteemi lahend. Tänu võrdusele (41) teame, et vektori m komponendid, mis asuvad kohtadel $j_{r+1}, \ldots, j_n$ on nullid. Seostest (40) järeldub, et ka kõik ülejäänud vektori m komponendid on nullid, mis tähendab, et m on nullvektor. Järelikult

$$l = u_1 k_1 + u_2 k_2 + \ldots + u_{n-r} k_{n-r},$$

mida oligi tarvis näidata. □

Näide 8.19 Lahendades homogeense lineaarvõrrandisüsteemi

$$\begin{cases} 2x_1 - 3x_2 + 5x_3 + 7x_4 = 0 \\ 4x_1 - 6x_2 + 2x_3 + 3x_4 = 0 \\ 2x_1 - 3x_2 - 11x_3 - 15x_4 = 0 \end{cases} \tag{42}$$

analoogiliselt sellega, kuidas lahendasime süsteemi (36) saame üldlahendiks vabade tundmatute kaudu

$$\begin{cases} x_1 = \frac{3}{2}x_2 - \frac{1}{16}x_4 \\ x_3 = -\frac{11}{8}x_4 \end{cases}. \tag{43}$$

Selle süsteemi lahendite fundamentaalsüsteemi saame kui anname vabadele tundmatutele x_2 ja x_4 kaks komplekti väärtusi mingi regulaarse teist järku ruutmaatriksi, nt. $\begin{pmatrix} 2 & 0 \\ 0 & 16 \end{pmatrix}$, ridadest ning arvutame kummalgi juhul võrduste (43) abil sõltuvate tundmatute x_1 ja x_3 väärtused:

$$\begin{aligned} d_1 &= (3, \mathbf{2}, 0, \mathbf{0}), \\ d_2 &= (-1, \mathbf{0}, -22, \mathbf{16}). \end{aligned}$$

Süsteemi (42) kõik lahendid avalduvad kujul $t_1 d_1 + t_2 d_2$, kus $t_1, t_2 \in \mathbb{R}$, s.t. et kõigi lahendite hulk on

$$L_h = \{t_1 d_1 + t_2 d_2 \mid t_1, t_2 \in \mathbb{R}\}.$$

8.5 Mittehomogeenne lineaarvõrrandisüsteem

Vaatleme üldist lineaarvõrrandisüsteemi

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad\qquad\qquad\qquad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{44}$$

Süsteemile (44) vastavaks homogeenseks lineaarvõrrandisüsteemiks nimetatakse süsteemi

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0, \end{cases} \tag{45}$$

mis on saadud süsteemist (44) kõigi vabaliikmete asendamisel nullidega. Meenutame, et maatrikskujul võime need kaks süsteemi kirja panna järgmiselt: $A\overline{x} = \overline{b}$ ja $A\overline{x} = \overline{0}$. Osutub, et nende kahe süsteemi lahendid on omavahel tihedalt seotud.

Kui U on vektorruumi V alamruum ja $v \in V$, siis tähistatakse

$$v + U := \{v + u \mid u \in U\}.$$

Tähistame süsteemi (44) kõigi lahendite hulka tähega L ja süsteemi (45) kõigi lahendite hulka sümboliga L_h.

Teoreem 8.20 *Süsteemide (44) ja (45) lahendihulkade L ja L_h vahel kehtib seos*

$$\boxed{L = d_* + L_h,}$$

kus $d_* \in L$ on süsteemi (44) mistahes lahend.

Tõestus. Olgu $d_* \in L$ süsteemi (44) suvaline lahend.

Näitame, et $d_* + L_h \subseteq L$. Kui $l \in L_h$, siis

$$A(\overline{d_* + l}) = A(\overline{d_*} + \overline{l}) = A\overline{d_*} + A\overline{l} = \overline{b} + \overline{0} = \overline{b},$$

mis tähendab, et $d_* + l \in L$. Seega $d_* + L_h \subseteq L$.

Võtame nüüd vektori $k \in L$. Siis

$$A(\overline{k - d_*}) = A(\overline{k} - \overline{d_*}) = A\overline{k} - A\overline{d_*} = \overline{b} - \overline{b} = \overline{0}$$

ehk $k - d_* \in L_h$. Järelikult $k = d_* + (k - d_*) \in d_* + L_h$, millega oleme näidanud, et $L \subseteq d_* + L_h$. □

Märkus 8.21 Teoreem 8.20 sõnastatakse tihti kujul: *mittehomogeense lineaarvõrrandisüsteemi üldlahend on võrdne selle süsteemi mingi erilahendi ja vastava homogeense lineaarvõrrandisüsteemi üldlahendi summaga.*

Näide 8.22 Vaatleme jälle lineaarvõrrandisüsteemi

$$\begin{cases} 2x_1 - 3x_2 + 5x_3 + 7x_4 = 1 \\ 4x_1 - 6x_2 + 2x_3 + 3x_4 = 2 \\ 2x_1 - 3x_2 - 11x_3 - 15x_4 = 1. \end{cases} \tag{46}$$

Sellele süsteemile vastava homogeense lineaarvõrrandisüsteemi (42) lahendite fundamentaalsüsteem on $d_1 = (3, 2, 0, 0), d_2 = (-1, 0, -22, 16)$. Nagu nägime näites 8.10 on süsteemi (46) üheks erilahendiks $d_* = (\frac{1}{2}, 0, 0, 0)$. Seega võime öelda, et süsteemi (46) kõigi lahendite hulk on

$$L = d_* + L_h = \{d_* + t_1 d_1 + t_2 d_2 \mid t_1, t_2 \in \mathbb{R}\}.$$

Teiste sõnadega: süsteemi (46) lahendid on kujul $d_* + t_1 d_1 + t_2 d_2$, kus $t_1, t_2 \in \mathbb{R}$.

9 Polünoomid

Lugeja on kindlasti tuttav polünoomidega, mille kordajateks on reaalarvud. Käesolevas peatükis vaatleme polünoome üle ringide. Alustuseks konstrueerime polünoomide ringi.

9.1 Polünoomide ring

Olgu R ring. Vaatleme kõigi selliste jadade hulka, mille komponendid kuuluvad ringi R ja mille komponendid on mingist kohast alates kõik võrdsed ringi R nullelemendiga. Tähistame selle hulga sümboliga $R[X]$. Seega

$$R[X] = \bigcup_{n\in\mathbb{N}\cup\{0\}} \{(a_0, a_1, \ldots, a_n, 0, 0, \ldots) \mid a_0, a_1, \ldots, a_n \in R\}.$$

Kaks hulka $R[X]$ kuuluvat jada on võrdsed parajasti siis, kui nende vastavad komponendid on võrdsed.

Definitsioon 9.1 Hulka $R[X]$ kuuluvate jadade $a = (a_0, a_1, a_2, \ldots)$ ja $b = (b_0, b_1, b_2, \ldots)$ **summa** defineeritakse võrdusega

$$a + b := c = (c_0, c_1, c_2, \ldots),$$

kus $c_k = a_k + b_k$ iga $k \in \mathbb{N} \cup \{0\}$ korral, ja **korrutis** defineeritakse võrdusega

$$ab := d = (d_0, d_1, d_2, \ldots),$$

kus

$$d_k = a_0b_k + a_1b_{k-1} + \ldots + a_{k-1}b_1 + a_kb_0 = \sum_{i+j=k} a_ib_j$$

iga $k \in \mathbb{N} \cup \{0\}$ korral.

Teoreem 9.2 *Hulk $R[X]$ on eelpooldefineeritud tehete suhtes ring. Kui R on kommutatiivne, siis ka ring $R[X]$ on kommutatiivne.*

Tõestus. Lihtne on aru saada, et kui jadade a ja b komponendid on mingist kohast alates nullid, siis on seda ka jadade $a + b$ ja ab komponendid. Seega on liitmine ja korrutamine algebralised tehted hulgal $R[X]$.

Jadade liitmine on assotsiatiivne ja kommutatiivne tänu sellele, et liitmine on defineeritud komponenthaaval ja ringi R elementide liitmine on assotsiatiivne ja kommutatiivne. Nullelemendiks on jada, mille kõik komponendid on nullid. Jada $a = (a_0, a_1, a_2, \ldots)$ vastandelemendiks on jada $-a = (-a_0, -a_1, -a_2, \ldots)$.

Kui $a = (a_0, a_1, a_2, \ldots) \in R[X]$ on suvaline, siis $(1, 0, 0, \ldots) \cdot a = (d_0, d_1, d_2, \ldots)$, kus

$$d_k = 1 \cdot a_k + 0 \cdot a_{k-1} + \ldots + 0 \cdot a_1 + 0 \cdot a_0 = a_k$$

iga $k \in \mathbb{N}\cup\{0\}$ korral. Seega $(1, 0, 0, \ldots)\cdot a = a$ ja analoogiliselt $a\cdot(1, 0, 0, \ldots) = a$, mis tähendab, et jada $(1, 0, 0, \ldots)$ on ringi $R[X]$ ühikelement.

Veendume, et korrutamine on assotsiatiivne. Olgu

$$\begin{aligned} a &= (a_0, a_1, a_2, \ldots), \\ b &= (b_0, b_1, b_2, \ldots), \\ c &= (c_0, c_1, c_2, \ldots), \\ ab &= (d_0, d_1, d_2, \ldots), \\ (ab)c &= (e_0, e_1, e_2, \ldots). \end{aligned}$$

Paneme tähele, et

$$\begin{aligned}\sum_{i+j+l=m} a_i b_j c_l &= \sum_{i+j=m} a_i b_j c_0 + \sum_{i+j=m-1} a_i b_j c_1 + \ldots + \sum_{i+j=0} a_i b_j c_m \\ &= \left(\sum_{i+j=m} a_i b_j\right) c_0 + \left(\sum_{i+j=m-1} a_i b_j\right) c_1 + \ldots + \left(\sum_{i+j=0} a_i b_j\right) c_m \\ &= \sum_{k+l=m} \left(\sum_{i+j=k} a_i b_j\right) c_l = \sum_{k+l=m} d_k c_l = e_m.\end{aligned}$$

Analoogiliselt saab näidata, et korrutise $a(bc)$ komponent indeksiga m on võrdne summaga $\sum_{i+j+l=m} a_i b_j c_l$. Järelikult $(ab)c = a(bc)$.

Näitame veel, et $(a+b)c = ac + bc$. Selleks olgu

$$\begin{aligned} a &= (a_0, a_1, a_2, \ldots), \\ b &= (b_0, b_1, b_2, \ldots), \\ c &= (c_0, c_1, c_2, \ldots), \\ a+b &= (d_0, d_1, d_2, \ldots), \\ (a+b)c &= (e_0, e_1, e_2, \ldots), \\ ac &= (u_0, u_1, u_2, \ldots), \\ bc &= (v_0, v_1, v_2, \ldots), \\ ac+bc &= (w_0, w_1, w_2, \ldots). \end{aligned}$$

Siis

$$\begin{aligned} e_k &= \sum_{i+j=k} d_i c_j = \sum_{i+j=k} (a_i + b_i) c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j, \\ w_k &= u_k + v_k = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j. \end{aligned}$$

Kuna $e_k = w_k$ iga $m \in \mathbb{N} \cup \{0\}$ korral, siis kehtibki $(a+b)c = ac+bc$. Võrduse $a(b+c) = ac+bc$ saab tõestada analoogiliselt. Seega on $R[X]$ ring.

Olgu nüüd R kommutatiivne ring ja $a = (a_0, a_1, a_2, \ldots), b = (b_0, b_1, b_2, \ldots) \in R[X]$. Siis $\sum_{i+j=k} a_i b_j = \sum_{j+i=k} b_j a_i$, millest järeldub, et $ab = ba$. □

Definitsioon 9.3 Ringi $R[X]$ nimetatakse **polünoomide ringiks üle ringi** R ning tema elemente nimetatakse **polünoomideks**.

Lause 9.4 *Hulk $R' = \{(r, 0, 0, \ldots) \mid r \in R\} \subseteq R[X]$ on ring definitsioonis 9.1 defineeritud tehete suhtes. See ring on isomorfne ringiga R.*

Tõestus. Lihtne on veenduda, et R' on ring. Samuti ei ole keeruline näha, et kujutus $\varphi : R \to R'$, mis on defineeritud võrdusega

$$\varphi(r) := (r, 0, 0, \ldots),$$

$a \in R$, on ringide isomorfism. □

Arvestades lauset 9.4 samastatakse jadad $(r, 0, 0, \ldots)$ ringi R elemendiga r.

Tähistame nüüd ringi $R[X]$ elemendi $(0,1,0,0,\ldots)$ sümboliga X:

$$X = (0,1,0,0,\ldots).$$

Kasutades korrutamise definitsiooni saame arvutada, et

$$\begin{aligned} X^1 &= (0,1,0,0,0,\ldots), \\ X^2 &= (0,0,1,0,0,\ldots), \\ X^3 &= (0,0,0,1,0,\ldots), \end{aligned}$$

jne. Matemaatilise induktsiooni abil saab näidata, et iga $n \in \mathbb{N}$ korral on X^n selline jada, mille komponent kohal $n+1$ on 1 (s.t. ringi R ühikelement) ja kõik ülejäänud komponendid on nullid. Kokkuleppeliselt loetakse, et $X^0 = (1,0,0,\ldots)$.

Olgu nüüd $f = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots)$ suvaline nullist erinev polünoom ringist $R[X]$ ja olgu a_n polünoomi f kui jada viimane nullist erinev komponent. Kuna

$$\begin{aligned} a_0 &= (a_0,0,0,0,\ldots), \\ a_1X &= (0,a_1,0,0,\ldots), \\ a_2X^2 &= (0,0,a_2,0,\ldots) \end{aligned}$$

ja nii edasi, siis on polünoom f esitatav kujul

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n.$$

Harilikult esitataksegi polünoome just sellisel kujul. Liidetavaid $a_0, a_1X, a_2X^2, \ldots, a_nX^n$ nimetatakse polünoomi f **liikmeteks**, liiget a_0 tema **vabaliikmeks** ja liiget a_nX^n tema **pealiikmeks**. Elemente $a_0, a_1, \ldots, a_n$ nimetatakse **polünoomi kordajateks**. Polünoomi $X \in R[X]$ nimetatakse **muutujaks** ning ringi $R[X]$ kohta öeldakse ka, et see on **polünoomide ring üle ringi** R **muutuja** X **suhtes**. Nullpolünoomi pealiige ei ole defineeritud. Polünoomi, mille pealiikmel on kuju X^n, s.t., mille pealiikme kordaja on 1, nimetatakse **unitaarseks polünoomiks**.

Kui $f \neq 0$ ja tal on kuju

$$f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n,$$

kusjuures $a_n \neq 0$, siis öeldakse, et polünoomi f **aste** on n. Nullpolünoomi astmeks loetakse $-\infty$. Polünoomi f astet tähistatakse sümboliga $\deg(f)$.

Polünoomi $f \in R[X]$ aste on 0 parajasti siis, kui $f = a_0 \neq 0$, s.t. kui f on nullist erinev ringi R element. Polünoome kujul $f = a_0 \in R$ kutsutakse **konstantseteks polünoomideks**. Kui $\deg(f) = 1$, siis öeldakse, et f on **lineaarpolünoom**. Kui $\deg(f) = 2$, siis öeldakse, et f on **ruutpolünoom**.

Mistahes polünoomide $f, g \in R[X]$ korral järeldub liitmise definitsioonist, et

$$\boxed{\deg(f+g) \leqslant \max(\deg(f), \deg(g)).} \tag{47}$$

Võib juhtuda, et polünoomide summa aste on rangelt väiksem liidetavate astmetest. Näiteks kui $f = 1 + 2X^2$ ja $g = 3 + X - 2X^2$, siis $\deg(f+g) = \deg(4+X) = 1$.

Definitsioon 9.5 Ringi R nullist erinevaid elemente a ja b nimetatakse **nullitegureiks**, kui $ab = 0$. Ring on **nullitegureita**, kui temas ei ole nullitegureid.

Lause 9.6 *Korpuses ei ole nullitegureid.*

TÕESTUS. Olgu K korpus ja oletame vastuväiteliselt, et $a, b \in K$ on nullist erinevad elemendid, mille korral $ab = 0$. Korrutades selle võrduse pooled paremalt elemendiga b^{-1}, saame $a = a(bb^{-1}) = (ab)b^{-1} = 0b^{-1} = 0$, mis on vastuolus eeldusega. □

Ka ringis $\mathbb{Z}$ ei ole nullitegureid. Samas näiteks ringis $\mathbb{Z}_6$ nullitegurid leiduvad: $\overline{2} \cdot \overline{3} = \overline{0}$, kuigi $\overline{2} \neq \overline{0}$ ja $\overline{3} \neq \overline{0}$.

Uurime, kuidas on polünoomide korrutise aste seotud tegurite astmetega.

Lause 9.7 *Mistahes ringi R ja nullist erinevate polünoomide $f, g \in R[X]$ korral*

$$\boxed{\deg(fg) \leqslant \deg(f) + \deg(g).}$$

Kui R on nullitegureita ring, siis

$$\boxed{\deg(fg) = \deg(f) + \deg(g).}$$

TÕESTUS. Olgu $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$ ja $g = (b_0, b_1, \ldots, b_m, 0, \ldots)$, kus a_n ja b_m on viimased nullist erinevad komponendid. Siis $\deg(f) = n$ ja $\deg(g) = m$. Olgu $fg = (d_0, d_1, d_2, \ldots)$. Definitsiooni 9.1 põhjal $d_k = \sum_{i+j=k} a_i b_j$ iga $k \in \mathbb{N} \cup \{0\}$ korral. Kui $k > n + m$, siis kõik liidetavad summas $\sum_{i+j=k} a_i b_j$ on nullid, mis tähendab, et $d_k = 0$. Seega viimane nullist erinev komponent jadas fg peab olema d_l, mille korral $l \leqslant n+m$. Järelikult $\deg(fg) = l \leqslant n+m = \deg(f)+\deg(g)$. Kuna $d_{n+m} = \sum_{i+j=n+m} a_i b_j = a_n b_m$, siis nullitegureita ringi R korral $d_{n+m} \neq 0$, sest $a_n, b_m \neq 0$. See tähendab, et $\deg(fg) = n + m = \deg(f) + \deg(g)$. □

Lause 9.7 abil saame lihtsasti tõestada järgmise tulemuse.

Teoreem 9.8 *Kui ring R on nullitegureita, siis ka polünoomide ring $R[X]$ on nullitegureita.*

TÕESTUS. Kui $f, g \in R[X]$ on nullist erinevad polünoomid, siis $\deg(f) \geqslant 0$ ja $\deg(g) \geqslant 0$. Järelikult $\deg(fg) = \deg(f) + \deg(g) \geqslant 0$, mis tähendab, et ka fg ei ole nullpolünoom. □

Selle teoreemi põhjal võib öelda, et nii ring $\mathbb{Z}[X]$ kui ka ringid $K[X]$, kus K on korpus (nt. $\mathbb{Q}$, $\mathbb{R}$ või $\mathbb{C}$), on nullitegureita.

Teeme nüüd kindlaks, millised on polünoomide ringi pööratavad elemendid. Ringi elementi nimetatakse **pööratavaks**, kui tal leidub pöördelement selle ringi korrutamistehte suhtes.

Lause 9.9 *Olgu R nullitegureita ring, milles on vähemalt kaks elementi. Siis polünoomide ringi $R[X]$ pööratavad elemendid on parajasti ringi R pööratavad elemendid (vaadelduna konstantsete polünoomidena).*

TÕESTUS. On selge, et kui $a \in R$ on pööratav, siis on ta pööratav ka kui konstantne polünoom.

Oletame nüüd, et $f \in R[X]$ on pööratav polünoom. Siis leidub polünoom $g \in R[X]$ nii, et $fg = 1$. On selge, et f ja g ei ole nullpolünoomid, sest muidu oleks nende korrutis nullpolünoom, mis erineb polünoomist 1 (vt. märkust 4.18). Oletame, et $\deg(f) \geqslant 1$. Siis

$$0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g) \geqslant 1,$$

sest $\deg(g) \geqslant 0$. See vastuolu näitab, et $\deg(f) = 0$, s.t. et f on konstantne polünoom. Analoogiliselt on g konstantne polünoom ja seega f on pööratav ringis R. □

Järeldus 9.10 *Kui K on korpus, siis ringi $K[X]$ pööratavad elemendid on parajasti nullist erinevad konstantsed polünoomid.*

TÕESTUS. Meenutame, et korpuses on vähemalt kaks elementi ja kõik nullist erinevad elemendid on pööratavad. □

Näide 9.11 Ringis $\mathbb{R}[X]$ on pööratavad elemendid polünoomid kujul $f = c$, kus $c \in \mathbb{R} \setminus \{0\}$. Ringis $\mathbb{Z}[X]$ on pööratavateks polünoomideks konstantsed polünoomid 1 ja -1.

9.2 Polünoomide jäägiga jagamine

Nagu hästi teada, saab iga täisarvu jagada jäägiga naturaalarvuga. Tuleb välja, et midagi sarnast saab teha ka polünoomidega.

Teoreem 9.12 *Olgu R nullitegureita ring, milles on vähemalt kaks elementi, ning olgu $f, g \in R[X]$, kusjuures polünoomi g pealiikme kordaja on pööratav ringis R. Siis leiduvad üheselt määratud polünoomid $q, r \in R[X]$ nii, et*

$$f = gq + r \quad ja \quad \deg(r) < \deg(g).$$

TÕESTUS. Olgu R nullitegureita ring ja olgu

$$g = b_m X^m + \ldots + b_1 X + b_0 \in R[X]$$

polünoom, mille pealiikme kordaja b_m on pööratav ringis R. Muuhulgas tähendab see, et g ei ole nullpolünoom ja $m = \deg(g) \geqslant 0$. Tõestame, et iga $f \in R[X]$ jaoks leiduvad sellised $q, r \in R[X]$, et $f = gq + r$ ja $\deg(r) < \deg(g)$. Teeme seda induktsiooniga polünoomi f astme järgi.

Kui $f = 0$, siis sobivateks polünoomideks on $q = r = 0$. Kui $\deg(f) = 0$, siis f on nullist erinev konstantne polünoom, $f = a_0 \in R \setminus \{0\}$. Sel juhul, kui g on mittekonstantne polünoom, siis võib võtta $q = 0$ ja $r = f$. Kui aga $g = b_0 \in R \setminus \{0\}$ ($b_0 \neq 0$, sest g pealiikme kordaja on pööratav), siis

$$a_0 = b_0(b_0^{-1}a_0)$$

ja me võime võtta $r = 0$, $q = b_0^{-1}a_0$. Sellega oleme tõestanud induktsiooni aluse.

Teeme nüüd induktsiooni sammu. Eeldame, et polünoomi

$$f = a_n X^n + \ldots + a_1 X + a_0 \in R[X]$$

aste $n > 0$ ja iga polünoomi $k \in R[X]$ jaoks, mille aste on väiksem kui n, leiduvad sellised $q, r \in R[X]$, et $k = gq + r$ ja $\deg(r) < \deg(g)$. On kaks võimalust.

1) $\deg(f) < \deg(g)$. Siis võib võtta $q = 0$ ja $r = f$.

2) $\deg(f) \geqslant \deg(g)$. Siis $n \geqslant m$. Olgu

$$g_1 := g\left(b_m^{-1}a_n X^{n-m}\right) \in R[X].$$

Siis g_1 on polünoom, mille pealiige on $a_n X^n$, s.t. sama, mis polünoomi f pealiige. Järelikult polünoomi

$$f_1 := f - g_1$$

aste on madalam kui polünoomi f aste n. Rakendades induktsiooni eeldust saab leida sellised $q_1, r \in R[X]$, et $f_1 = gq_1 + r$ ja $\deg(r) < \deg(g)$. Siis aga

$$f = g_1 + f_1 = g\left(b_m^{-1}a_n X^{n-m}\right) + gq_1 + r = g\left(b_m^{-1}a_n X^{n-m} + q_1\right) + r.$$

Tähistades $q := b_m^{-1}a_nX^{n-m} + q_1 \in R[X]$ olemegi saanud sellised q ja r nagu vaja.

Tõestuse lõpetamiseks tuleb veel näidata, et q ja r on üheselt määratud f ja g poolt. Selleks oletame, et

$$f = gq_1 + r_1,\ \deg(r_1) < \deg(g) \quad \text{ja} \quad f = gq_2 + r_2,\ \deg(r_2) < \deg(g).$$

Siis $gq_1 + r_1 = gq_2 + r_2$, millest saame võrduse

$$g(q_1 - q_2) = r_2 - r_1.$$

Kuna $\deg(r_1) < \deg(g)$ ja $\deg(r_2) < \deg(g)$, siis $\deg(r_2 - r_1) < \deg(g)$ tänu võrratusele (47). Lause 9.7 põhjal

$$\deg(g(q_1 - q_2)) = \deg(g) + \deg(q_1 - q_2).$$

Järelikult

$$\deg(r_2 - r_1) = \deg(g) + \deg(q_1 - q_2).$$

Et $\deg(g) \geqslant 0$, siis viimane võrdus saab kehtida vaid juhul, kui $\deg(q_1 - q_2) = \deg(r_2 - r_1) = -\infty$. See tähendab, et $q_1 - q_2 = r_2 - r_1 = 0$ ehk $q_1 = q_2$ ja $r_1 = r_2$. □

Teoreemis 9.12 kirjeldatud polünoome q ja r nimetatakse vastavalt **jagatiseks** ja **jäägiks**, mis tekivad polünoomi f jagamisel polünoomiga g.

9.3 Jaguvus nullitegureita ringides

Kogu käesoleva paragrahvi jooksul olgu R kommutatiivne nullitegureita ring.

Definitsioon 9.13 Olgu $a, b \in R$. Öeldakse, et element a **jagab** elementi b (ja tähistatakse $a \mid b$), kui leidub selline $c \in R$, et $ac = b$.

Paneme tähele, et element $a \in R$ on pööratav, parajasti siis, kui a jagab ringi R ühikelementi. Lihtne on veenduda, et kehtib järgmine lause.

Lause 9.14 *Jaguvusseosel ringis R on järgmised omadused.*

1. *Kui $a \mid b$ ja $b \mid c$, siis $a \mid c$;*
2. *kui $a \mid b$ ja $a \mid c$, siis $a \mid b \pm c$;*
3. *kui $a \mid b$, siis $a \mid bc$*

iga $a, b, c \in R$ korral.

Definitsioon 9.15 Öeldakse, et ringi R elemendid a ja b on **assotsieeritud** (ja tähistatakse $a \sim b$), kui $a \mid b$ ja $b \mid a$.

Lause 9.16 *Olgu $a, b \in R \setminus \{0\}$. Elemendid a ja b on assotsieeritud parajasti siis, kui leidub mingi pööratav element $u \in R$ nii, et $a = bu$.*

Tõestus. Tarvilikkus. Eeldame, et $a \mid b$ ja $b \mid a$. Siis leiduvad $c, d \in R$ nii, et $ac = b$ ja $bd = a$. Järelikult $a = acd$, kust $a(1 - cd) = 0$. Kuna $a \neq 0$ ja ring on nullitegureita, siis $1 - cd = 0$ ehk $1 = cd$. Seega d on pööratav.
Piisavus. Olgu $a = bu$, kus u on pööratav. Siis $b = au^{-1}$. Järelikult $a \mid b$ ja $b \mid a$. □

Näide 9.17 1. Ringis $\mathbb{Z}$ on elemendid a ja b assotsieeritud parajasti siis, kui $a = b$ või $a = -b$, sest ringi $\mathbb{Z}$ pööratavad elemendid on 1 ja -1.

2. Korpuses on mistahes kaks nullist erinevat elementi a ja b assotsieeritud, sest $a(a^{-1}b) = b$, kus $a^{-1}b$ on pööratav.

3. Kui $f \in R[X]$ ja c on pööratav element ringis R, siis polünoomid f ja fc on assotsieeritud. Näiteks ringis $\mathbb{R}[X]$ on polünoomid $4X^3 + 6X - 10$ ja $2X^3 + 3X - 5$ assotsieeritud.

Definitsioon 9.18 Elementi $d \in R$ nimetatakse elementide a ja b **suurimaks ühisteguriks** (ja tähistatakse $d = \text{SÜT}(a, b)$), kui

1. $d \mid a$ ja $d \mid b$;
2. kui $d' \in R$, $d' \mid a$ ja $d' \mid b$, siis $d' \mid d$.

Lause 9.19 *Kui $d \in R$ on elementide a ja b suurim ühistegur ja $d \sim c$, siis ka c on elementide a ja b suurim ühistegur.*

Tõestus. Olgu $d = \text{SÜT}(a, b)$ ja $d \sim c$. Siis $d \mid c$ ja $c \mid d$. Veendume, et c rahuldab elementide a ja b suurima ühisteguri definitsiooni tingimusi.

1. Kuna $c \mid d$, $d \mid a$ ja $d \mid b$, siis ka $c \mid a$ ja $c \mid b$ lause 9.14(1) põhjal.
2. Oletame, et $d' \in R$ on selline, et $d' \mid a$ ja $d' \mid b$. Siis $d' \mid d$. Kuna $d' \mid d$ ja $d \mid c$, siis $d' \mid c$. □

Näide 9.20 Täisarvudel 6 ja -9 on kaks suurimat ühistegurit ringis $\mathbb{Z}$, need on arvud 3 ja -3.

9.4 Polünoomide suurim ühistegur

Näitame, kuidas leida polünoomide suurimat ühistegurit, kui nende polünoomide kordajad on mingist korpusest. Osutub, et sarnaselt täisarvudega saab selleks kasutada nn. Eukleidese algoritmi.

Teoreem 9.21 *Mistahes kahel polünoomil üle korpuse K leidub suurim ühistegur.*

Tõestus. Olgu $f, g \in K[X]$. Kui $f = 0$, siis definitsiooni põhjal $\text{SÜT}(f, g) = g$ ja kui $g = 0$, siis $\text{SÜT}(f, g) = f$. Eeldame nüüd, et $f \neq 0$ ja $g \neq 0$. Jagame polünoomi f jäägiga polünoomiga g:

$$f = gq_1 + r_1, \qquad \deg(r_1) < \deg(g).$$

(Seda saame teha tänu teoreemile 9.12.) Kui $r_1 = 0$, siis $g \mid f$ ja seega $\text{SÜT}(f, g) = g$. Kui $r_1 \neq 0$, siis jagame polünoomi g polünoomiga r_1:

$$g = r_1q_2 + r_2, \qquad \deg(r_2) < \deg(r_1).$$

Kui $r_2 = 0$, siis lõpetame; vastasel juhul jagame polünoomi r_1 polünoomiga r_2:

$$r_1 = r_2q_3 + r_3, \qquad \deg(r_3) < \deg(r_2).$$

Niimoodi jätkame senikaua kui saame mingil sammul jäägiks $r_{n+1} = 0$. Varem või hiljem peab see juhtuma, sest $\deg(g) > \deg(r_1) > \deg(r_2) > \ldots$ ja ei leidu lõpmatuid kahanevaid naturaalarvujadasid. Osutub, et suurimaks ühisteguriks on viimane nullist erinev jääk r_n. Tehtud sammud võib kokku võtta järgmise tabelina:

$$\begin{array}{rcll} f & = & gq_1 + r_1, & \deg(r_1) < \deg(g), \\ g & = & r_1q_2 + r_2, & \deg(r_2) < \deg(r_1), \\ r_1 & = & r_2q_3 + r_3, & \deg(r_3) < \deg(r_2), \\ & \dots & & \\ r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1} & \deg(r_{n-1}) < \deg(r_{n-2}), \\ r_{n-2} & = & r_{n-1}q_n + r_n & \deg(r_n) < \deg(r_{n-1}), \\ r_{n-1} & = & r_nq_{n+1} + 0. & \end{array} \tag{48}$$

Näitame, et $r_n = \text{SÜT}(f, g)$. Selleks kontrollime definitsiooni tingimusi.

1. Tabeli (48) viimasest reast näeme, et $r_n \mid r_{n-1}$. Kuna $r_n \mid r_n$ ja $r_n \mid r_{n-1}$, siis tabeli eelviimasest reast saame, et $r_n \mid r_{n-2}$. Kuna $r_n \mid r_{n-1}$ ja $r_n \mid r_{n-2}$, siis tabeli üle-eelviimasest reast saame, et $r_n \mid r_{n-3}$. Niimoodi ülespoole liikudes näeme lõpuks, et $r_n \mid g$ ja $r_n \mid f$.

2. Oletame nüüd, et h on selline polünoom, et $h \mid f$ ja $h \mid g$. Tabeli esimese rea põhjal $h \mid f - gq_1 = r_1$. Teisest reast saame, et $h \mid r_2$. Järjest allapoole liikudes näeme lõpuks, et $h \mid r_n$. □

Suurima ühisteguri leidmise algoritmi, mida kirjeldasime teoreemi 9.21 tõestuses, nimetatakse **Eukleidese algoritmiks**.

Lause 9.22 *Kui K on korpus, $f, g \in K[X]$ ja $d = \text{SÜT}(f, g)$, siis leiduvad sellised $u, v \in K[X]$, et*

$$uf + vg = d.$$

TÕESTUS. Olgu polünoomide f ja g suurim ühistegur leitud Eukleidese algoritmi abil, s.t. kehtigu võrdused (48) ja olgu $d = r_n$. Liikudes tabelis altpoolt üles saame

$$\begin{array}{rcl} r_n & = & r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n \\ & = & r_{n-3}(-q_n) + r_{n-2}(1 + q_{n-1}q_n) = \ldots = fu + gv. \end{array}$$

□

9.5 Polünoomi juured

Käesolevas paragrahvis eeldame kõikjal, et R on nullitegureita kommutatiivne ring, milles on vähemalt kaks elementi.

Definitsioon 9.23 Olgu R nullitegureita kommutatiivne ring,

$$f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$$

polünoom ringist $R[X]$ ja $c \in R$. Ringi R elementi

$$a_0c^n + a_1c^{n-1} + \ldots + a_{n-1}c + a_n$$

nimetatakse polünoomi $f(X)$ **väärtuseks** kohal c ja tähistatakse $f(c)$.

Elementi $c \in R$ nimetatakse polünoomi $f(X)$ **juureks**, kui $f(c) = 0$.

Teoreem 9.24 (Bezout' teoreem)[7] *Polünoomi $f(X) \in R[X]$ väärtus kohal $c \in R$ on võrdne jäägiga, mis tekib polünoomi $f(X)$ jagamisel polünoomiga $X - c$.*

[7] Étienne Bézout (1730–1783) — prantsuse matemaatik

TÕESTUS. Jagame polünoomi $f(X) \in R[X]$ jäägiga lineaarpolünoomiga $X - c$, kus $c \in R$:

$$f(X) = (X - c)q(X) + r(X), \qquad \deg(r(X)) < \deg(X - c) = 1.$$

Kuna $\deg(r(X)) < 1$, siis $r(X) = r \in R$ on konstantne polünoom. Kui kaks polünoomi (antud juhul $f(X)$ ja $(X - c)q(X) + r(X)$) on võrdsed, siis on võrdsed ka nende väärtused kohal c. Järelikult

$$f(c) = (c - c) \cdot q(c) + r = 0 + r = r.$$

□

Bezout' teoreemist ja jaguvuse definitsioonist järeldub järgmine tulemus.

Järeldus 9.25 *Element $c \in R$ on polünoomi $f(X) \in R[X]$ juur parajasti siis, kui $X - c \mid f(X)$.*

Polünoomi väärtuse leidmiseks kohal c võib muidugi kasutada definitsiooni 9.23, kuid tuleb välja, et on ka veidi lihtsam võimalus. Olgu polünoomi $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$ ja polünoomi $X - c$ jagatis

$$q(X) = b_0X^{n-1} + b_1X^{n-2} + \ldots + b_{n-2}X + b_{n-1}$$

ja jääk $r \in R$. Siis kehtib võrdus

$$f(X) = (X - c)q(X) + r.$$

Selle võrduse paremal poolel on polünoom

$$b_0X^n + (b_1 - cb_0)X^{n-1} + (b_2 - cb_1)X^{n-2} + \ldots + (b_{n-1} - cb_{n-2})X + (r - cb_{n-1}).$$

See polünoom peab võrduma polünoomiga $f(X)$, mis tähendab, et X vastavate astmete kordajad peavad olema samad. Seega peavad kehtima võrdused

$$\begin{array}{rcl} a_0 &=& b_0, \\ a_1 &=& b_1 - cb_0, \\ a_2 &=& b_2 - cb_1, \\ &\ldots& \\ a_{n-1} &=& b_{n-1} - cb_{n-2}, \\ a_n &=& r - cb_{n-1}, \end{array} \qquad \text{ehk} \qquad \begin{array}{rcl} b_0 &=& a_0, \\ b_1 &=& a_1 + cb_0, \\ b_2 &=& a_2 + cb_1, \\ &\ldots& \\ b_{n-1} &=& a_{n-1} + cb_{n-2}, \\ r &=& a_n + cb_{n-1}. \end{array}$$

Jagatise $q(X)$ ja jäägi r leidmist nende võrduste abil kutsutakse **Horneri**[8] **skeemiks**. Harilikult esitatakse Horneri skeem järgneva tabeli kujul:

$$\begin{array}{c|cccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ c & & cb_0 & cb_1 & \ldots & cb_{n-2} & cb_{n-1} \\ \hline & b_0 & b_1 & b_2 & \ldots & b_{n-1} & r \end{array}.$$

Selle tabeli teise rea elemendid saadakse kolmanda rea elementide korrutamisel c-ga ja joone all olevad elemendid saadakse joone kohal olevate elementide liitmisel. Tihti jäetakse selle tabeli teine rida üldse ära.

Polünoomi juure korral võib rääkida selle kordsusest.

[8] William George Horner (1786–1837) — inglise matemaatik

Definitsioon 9.26 Olgu k naturaalarv. Elementi $c \in R$ nimetatakse polünoomi $0 \neq f(X) \in R[X]$ **k-kordseks juureks**, kui $(X-c)^k \mid f(X)$, aga $(X-c)^{k+1} \nmid f(X)$ ringis $R[X]$.

Näide 9.27 Arv 1 on polünoomi $f(X) = (X-1)^2(X+2) = X^3 - 3X + 2 \in \mathbb{Z}[X]$ kahekordne juur ja arv -2 on selle polünoomi ühekordne juur.

Ilma tõestuseta mainime, et kehtib järgmine lause.

Lause 9.28 *Olgu $0 \neq f(X) \in R[X]$, kus R on nullitegureita kommutatiivne ring. Olgu $c_1, \ldots, c_m$ polünoomi $f(X)$ vastavalt $k_1, \ldots, k_m$-kordsed juured, mis on paarikaupa erinevad. Siis leidub selline polünoom $g(X) \in R[X]$, et*

$$f(X) = (X-c_1)^{k_1} \ldots (X-c_m)^{k_m} g(X),$$

kusjuures ükski elementidest $c_1, \ldots, c_m$ ei ole polünoomi $g(X)$ juur. Kui polünoomi $f(X)$ aste on n, siis

$$k_1 + \ldots + k_m \leqslant n.$$

Selle lause teine pool sõnastatakse tihti ka kujul: *polünoomi $f(X)$ juurte koguarv (kordsust arvestades) ei ületa selle polünoomi astet.*

Näide 9.29 Polünoomi $f(X) = X^4 - 4X^3 + 5X^2 - 4X + 4 \in \mathbb{R}[X]$ saab esitada kujul

$$f(X) = (X-2)^2(X^2+1).$$

Siit näeme, et sellel polünoomil on kahekordne juur 2. Kui vaatleksime seda polünoomi üle korpuse $\mathbb{C}$, siis oleks tal veel ka ühekordsed juured i ja $-i$.

9.6 Kordsete tegurite eraldamine

Selles paragrahvis vaatleme lihtsuse mõttes polünoome üle korpuse $\mathbb{R}$. Samasugused tulemused kehtivad siiski ka üldisemal juhul, muuhulgas korpuste $\mathbb{Q}$ ja $\mathbb{C}$ korral.

Definitsioon 9.30 Mittekonstantset polünoomi ringist $\mathbb{R}[X]$ nimetatakse **taandumatuks**, kui teda ei saa esitada kahe mittekonstantse polünoomi korrutisena.

Näide 9.31 Iga lineaarpolünoom $aX + b \in \mathbb{R}[X]$ (kus $a \neq 0$) on taandumatu. Polünoom $X^2 + 1 \in \mathbb{R}[X]$ on taandumatu. Polünoom $X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$ on taanduv.

Lihtne on näha, et kehtib järgmine tulemus.

Lause 9.32 *Iga mittekonstantse polünoomi ringis $\mathbb{R}[X]$ saab esitada taandumatute polünoomide korrutisena.*

Definitsioon 9.33 Olgu $f \in \mathbb{R}[X]$, olgu $p \in \mathbb{R}[X]$ taandumatu polünoom ja $k \in \mathbb{N}$. Polünoomi p nimetatakse polünoomi f **k-kordseks teguriks**, kui $p^k \mid f$, aga $p^{k+1} \nmid f$ ringis $\mathbb{R}[X]$.

Definitsioon 9.34 Olgu $f = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{R}[X]$. Polünoomi f **tuletiseks** nimetatakse polünoomi

$$f' = na_0X^{n-1} + (n-1)a_1X^{n-2} + \ldots + a_{n-1} \in \mathbb{R}[X].$$

Definitsioonist on näha, et kui $\deg(f) = n$, siis $\deg(f') = n - 1$.

Ilma tõestuseta märgime, et kehtib järgmine teoreem.

Teoreem 9.35 *Kui taandumatu polünoom $p \in \mathbb{R}[X]$ on polünoomi $f \in \mathbb{R}[X]$ k-kordne tegur, siis on ta tuletise f' $(k-1)$-kordne tegur.*

Olgu

$$f = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \in \mathbb{R}[X],$$

kus $k_1, \dots, k_m \in \mathbb{N}$, $p_1, \dots, p_m \in \mathbb{R}[X]$ on taandumatud polünoomid ja $\text{SÜT}(p_i, p_j) = 1$, kui $i \neq j$. On võimalik näidata, et siis polünoomil f teisi taandumatuid tegureid ei ole. Teoreemi 9.35 abil saab tõestada, et

$$\text{SÜT}(f, f') = p_1^{k_1 - 1} p_2^{k_2 - 1} \dots p_m^{k_m - 1}.$$

Siis $\text{SÜT}(f, f') \mid f$ ning f ja $\text{SÜT}(f, f')$ jagatiseks on polünoom

$$\frac{f}{\text{SÜT}(f, f')} = p_1 p_2 \dots p_m =: g,$$

millel on samad taandumatud tegurid nagu polünoomil f, aga kordsusega 1. Sellise polünoomi g leidmist nimetatakse polünoomi f **kordsete tegurite eraldamiseks**.

Niisiis: *polünoomi kordsete tegurite eraldamiseks tuleb see polünoom jagada tema ja tema tuletise suurima ühisteguriga.* Suurim ühistegur leitakse reeglina Eukleidese algoritmi abil.

Kui c on polünoomi f juur, siis taandumatu polünoom $X - c$ jagab nii polünoomi f kui ka polünoomi g. Seega c on ka polünoomi g juur. Kui meil õnnestub leida polünoomi g juured, siis oleme leidnud ka polünoomi f juured. Kuna üldiselt on polünoomi g aste väiksem kui polünoomi f aste, siis on juurte leidmine polünoomi g põhjal lihtsam kui esialgse polünoomi f põhjal.

10 Lineaarkujutused

10.1 Lineaarkujutuse definitsioon

Algebraliste struktuuride uurimisel on suur tähtsus tehteid säilitavatel kujutustel sama tüüpi struktuuride vahel. Meie vaatleme selliseid kujutusi vektorruumide korral.

Definitsioon 10.1 Olgu V_1 ja V_2 vektorruumid üle korpuse K. Kujutust $\varphi : V_1 \to V_2$ nimetatakse **lineaarkujutuseks**, kui

LK1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ iga $a, b \in V_1$ korral (s.t. φ säilitab liitmise);

LK2. $\varphi(ka) = k\varphi(a)$ iga $a \in V_1$ ja $k \in K$ korral (s.t. φ säilitab skalaaridega korrutamise).

Definitsioon 10.2 Lineaarkujutust vektorruumist V iseendasse nimetatakse vektorruumi V **lineaarteisenduseks**.

Kõigi lineaarkujutuste hulka vektorruumist V_1 vektorruumi V_2 tähistatakse sümboliga $\mathrm{Hom}(V_1, V_2)$. Vektorruumi V kõigi lineaarteisenduste hulka tähistatakse sümboliga $\mathrm{End}(V)$. (Hom tuleb sõnast "homomorfism", End sõnast "endomorfism".)

Näide 10.3 1. Iga vektorruumi V samasusteisendus 1_V on lineaarteisendus.

2. Mistahes vektorruumide V_1 ja V_2 korral on kujutus $V_1 \to V_2$, mis viib kõik V_1 vektorid V_2 nullvektoriks, lineaarkujutus. Sellist kujutust nimetatakse **nullkujutuseks** ja tähistatakse tihti sümboliga 0.

3. Olgu $A \in \mathrm{Mat}_{m,n}(K)$ fikseeritud maatriks. Kujutus $\varphi : K^n \to K^m$, mis on defineeritud võrdusega

$$\varphi(x) := Ax,$$

$x \in K^n$, on lineaarkujutus. Siin me samastame vektori $x \in K^n$ talle vastava veeruvektoriga.

4. Tasandi vabavektorite vektorruumi $\mathbb{E}_2$ üheks lineaarteisenduseks on teisendus, mis peegeldab iga vektorit fikseeritud koordinaatsüsteemi y-telje suhtes.

5. Kui defineerida polünoomi $a_nX^n + \ldots + a_1X + a_0 \in \mathbb{R}[X]$ ja reaalarvu k korrutis võrdusega $k(a_nX^n + \ldots + a_1X + a_0) := ka_nX^n + \ldots + ka_1X + ka_0$, siis on hulk $\mathbb{R}[X]$ vektorruum üle korpuse $\mathbb{R}$. Diferentseerimiskujutus

$$\varphi : \mathbb{R}[X] \to \mathbb{R}[X], \quad f(X) \mapsto f'(X),$$

on lineaarne.

Lineaarkujutuse definitsioonist järeldub, et lineaarkujutusel on veel teisigi omadusi.

Lause 10.4 *Olgu $\varphi : V_1 \to V_2$ lineaarkujutus. Siis*

1. $\varphi(0) = 0$;
2. $\varphi(-a) = -\varphi(a)$ *iga* $a \in V_1$ *korral.*
3. $\varphi(a-b) = \varphi(a) - \varphi(b)$ *iga* $a, b \in V_1$ *korral.*

Teiste sõnadega: lineaarkujutus säilitab nullelemendi, vastandelemendi võtmise ja lahutamise.

TÕESTUS. 1. Definitsiooni põhjal $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$. Liites selle võrduse mõlemale poolele $-\varphi(0)$ saamegi võrduse $0 = \varphi(0)$.

2. Kuna $\varphi(a) + \varphi(-a) = \varphi(a-a) = \varphi(0)$, siis $\varphi(-a) = -\varphi(a)$ iga $a \in V_1$ korral.

3. Tõepoolest, kui $a, b \in V_1$, siis

$$\varphi(a-b) = \varphi(a+(-b)) = \varphi(a) + \varphi(-b) = \varphi(a) + (-\varphi(b)) = \varphi(a) - \varphi(b).$$

□

Tuleb välja, et lineaarkujutuse defineerimiseks piisab, kui näitame ära, kuidas see kujutus tegutseb baasivektoritel.

Lause 10.5 *Olgu V_1 ja V_2 vektorruumid üle korpuse K, olgu $e = \{e_1, \ldots, e_n\}$ vektorruumi V_1 baas ja olgu $\psi : e \to V_2$ suvaline kujutus. Siis leidub lineaarkujutus $\varphi : V_1 \to V_2$ nii, et $\varphi(e_i) = \psi(e_i)$ iga $i \in \{1, \ldots, n\}$ korral.*

TÕESTUS. Defineerime kujutuse $\varphi : V_1 \to V_2$ järgmiselt:

$$\varphi(a) = \varphi\left(\sum_{i=1}^{n} a_i e_i\right) := \sum_{i=1}^{n} a_i \psi(e_i)$$

mistahes vektori $a = \sum_{i=1}^{n} a_i e_i$ korral. Kuna vektorruumi V_1 iga element a on tänu lausele 6.45 üheselt esitatav kujul $a = \sum_{i=1}^{n} a_i e_i$, siis on see definitsioon korrektne. On selge, et $\varphi(e_i) = \psi(e_i)$ iga $i \in \{1, \ldots, n\}$ korral.

Kujutus φ on lineaarkujutus, sest mistahes vektorite $a = \sum_{i=1}^{n} a_i e_i$ ja $b = \sum_{i=1}^{n} b_i e_i$ ning skalaari $k \in K$ korral

$$\begin{aligned}
\varphi\left(\sum_{i=1}^{n} a_i e_i + \sum_{i=1}^{n} b_i e_i\right) &= \varphi\left(\sum_{i=1}^{n} (a_i + b_i) e_i\right) = \sum_{i=1}^{n} (a_i + b_i)\psi(e_i) \\
&= \sum_{i=1}^{n} a_i \psi(e_i) + \sum_{i=1}^{n} b_i \psi(e_i) = \varphi\left(\sum_{i=1}^{n} a_i e_i\right) + \varphi\left(\sum_{i=1}^{n} b_i e_i\right), \\
\varphi\left(k \sum_{i=1}^{n} a_i e_i\right) &= \varphi\left(\sum_{i=1}^{n} (k a_i) e_i\right) = \sum_{i=1}^{n} (k a_i)\psi(e_i) = k \sum_{i=1}^{n} a_i \psi(e_i) = k\varphi\left(\sum_{i=1}^{n} a_i e_i\right).
\end{aligned}$$

□

10.2 Lineaarkujutuse tuum ja kujutis

Iga lineaarkujutusega on loomulikul viisil seotud kaks alamruumi.

Definitsioon 10.6 Lineaarkujutuse $\varphi : V_1 \to V_2$

1. **tuumaks** nimetatakse hulka

$$\operatorname{Ker} \varphi = \{a \in V_1 \mid \varphi(a) = 0\} \subseteq V_1,$$

2. **kujutiseks** nimetatakse hulka

$$\operatorname{Im} \varphi = \{\varphi(a) \mid a \in V_1\} \subseteq V_2.$$

Lause 10.7 *Olgu V_1 ja V_2 vektorruumid üle korpuse K. Lineaarkujutuse $\varphi : V_1 \to V_2$*

1. *tuum on vektorruumi V_1 alamruum,*
2. *kujutis on vektorruumi V_2 alamruum.*

TÕESTUS. Kuna $\varphi(0) = 0$, siis V_1 nullvektor kuulub hulka $\operatorname{Ker}\varphi$ ja V_2 nullvektor hulka $\operatorname{Im}\varphi$. Seega need hulgad on mittetühjad.

1. Olgu $a, b \in \operatorname{Ker}\varphi$ ja $k \in K$. Siis

$$\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$$

ja $\varphi(ka) = k\varphi(a) = k0 = 0$. Järelikult $a+b, ka \in \operatorname{Ker}\varphi$ ja $\operatorname{Ker}\varphi$ on V_1 alamruum.

2. Selle osa tõestusest jätame läbimõtlemiseks lugejale. □

Osutub, et tuuma põhjal saab kindlaks teha, millal on lineaarkujutus üksühene.

Lause 10.8 *Lineaarkujutus $\varphi : V_1 \to V_2$ on üksühene parajasti siis, kui* $\operatorname{Ker}\varphi = \{0\}$.

TÕESTUS. TARVILIKKUS. Olgu φ üksühene ja $a \in \operatorname{Ker}\varphi$. Kuna $\varphi(a) = 0 = \varphi(0)$, siis üksühesuse tõttu $a = 0$. Seega $\operatorname{Ker}\varphi \subseteq \{0\}$. Kuna vastupidine sisalduvus on ilmne, siis peabki kehtima võrdus $\operatorname{Ker}\varphi = \{0\}$.
PIISAVUS. Eeldame, et $\operatorname{Ker}\varphi = \{0\}$. Kehtigu võrdus $\varphi(a) = \varphi(b)$, $a, b \in V_1$. Siis

$$\varphi(a-b) = \varphi(a) - \varphi(b) = 0.$$

Järelikult $a - b \in \operatorname{Ker}\varphi = \{0\}$, s.t. $a - b = 0$ ehk $a = b$. Sellega oleme näidanud, et φ on üksühene. □

Lause 10.9 *Lineaarkujutus $\varphi : V_1 \to V_2$ on pealekujutus parajasti siis, kui* $\operatorname{Im}\varphi = V_2$.

TÕESTUS. See järeldub vahetult definitsioonidest. □

10.3 Lineaarkujutuse maatriks

Kui vektorruumides V_1 ja V_2 on fikseeritud mingid baasid, siis saab iga lineaarkujutusega $\varphi : V_1 \to V_2$ siduda teatud maatriksi.

Definitsioon 10.10 Olgu V_1 ja V_2 vektorruumid üle korpuse K, olgu $e = \{e_1, \ldots, e_n\}$ vektorruumi V_1 baas ja $e' = \{e'_1, \ldots, e'_m\}$ vektorruumi V_2 baas ning olgu $\varphi : V_1 \to V_2$ lineaarkujutus. **Lineaarkujutuse φ maatriksiks baaside e ja e' suhtes** nimetatakse maatriksit $A = (a_{ij}) \in \operatorname{Mat}_{m,n}(K)$, mille i-nda veeruvektori ($i \in \{1, \ldots, n\}$) komponendid on vektori $\varphi(e_i)$ koordinaadid baasi e' suhtes. Seda maatriksit tähistatakse sümboliga $A_\varphi^{e,e'}$.

Kui φ on vektorruumi V lineaarteisendus ja e on vektorruumi V baas, siis maatriksit $A_\varphi^{e,e}$ nimetatakse **lineaarteisenduse φ maatriksiks baasi e suhtes** ja tähistatakse A_φ^e.

Vastavalt sellele definitsioonile peavad lineaarkujutuse φ korral kehtima võrdused

$$\varphi(e_i) = a_{1i}e'_1 + \ldots + a_{mi}e'_m = \sum_{j=1}^{m} a_{ji}e'_j, \tag{49}$$

$i = 1, \ldots, n$.

Lineaarkujutuse maatriksi leidmiseks tuleb
1. leida vektorid $\varphi(e_1), \ldots, \varphi(e_n)$,
2. avaldada need baasi e' kaudu,
3. saadud koordinaate veergudesse paigutades moodustada maatriks A.

Näide 10.11 1. Samasusteisenduse maatriks mistahes baasi suhtes on ühikmaatriks.

2. Nullkujutuse maatriks misthes baaside suhtes on nullmaatriks.

3. Olgu tasandi vabavektorite vektorruumis $\mathbb{E}_2$ fikseeritud mingi ristbaas $e = \{\vec{i}, \vec{j}\}$. Vaatleme lineaarteisendust $\varphi : \mathbb{E}_2 \to \mathbb{E}_2$, mis seisneb vektorite peegeldamises y-telje suhtes. Kuna

$$\begin{aligned} \varphi(\vec{i}) &= -\vec{i} = (-1)\vec{i} + 0\vec{j}, \\ \varphi(\vec{j}) &= \vec{j} = 0\vec{i} + 1\vec{j}, \end{aligned}$$

siis

$$A_\varphi^e = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Tuleb välja, et lineaarkujutuse rakendamise vektorile võib taandada selle vektori koordinaatide veeru korrutamisele lineaarkujutuse maatriksiga. Vektori x koordinaatide veergu baasi $e = \{e_1, \ldots, e_n\}$ suhtes tähistame sümboliga $\overline{x}_e$. Seega

$$\overline{x}_e = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \iff x = x_1 e_1 + \ldots + x_n e_n.$$

Lause 10.12 *Olgu V_1 ja V_2 vektorruumid üle korpuse K, olgu e vektorruumi V_1 baas ja e' vektorruumi V_2 baas ning olgu $\varphi : V_1 \to V_2$ lineaarkujutus. Siis iga vektori $x \in V_1$ korral*

$$\boxed{\overline{\varphi(x)}_{e'} = A_\varphi^{e,e'} \overline{x}_e.}$$

Tõestus. Olgu $x = x_1 e_1 + \ldots + x_n e_n = \sum_{i=1}^n x_i e_i$, kus $x_1, \ldots, x_n \in K$, olgu $A_\varphi^{e,e'} = (a_{ij})$ ja $A_\varphi^{e,e'} \overline{x}_e = \begin{pmatrix} b_1 \\ \cdots \\ b_m \end{pmatrix}$. Kasutades φ lineaarsust, seoseid (49), summeerimise omadusi ja maatriksite korrutamise definitsiooni saame

$$\begin{aligned} \varphi(x) &= \varphi\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i \varphi(e_i) = \sum_{i=1}^n x_i \left(\sum_{j=1}^m a_{ji} e'_j\right) \\ &= \sum_{i=1}^n \sum_{j=1}^m x_i a_{ji} e'_j = \sum_{j=1}^m \left(\sum_{i=1}^n a_{ji} x_i\right) e'_j = \sum_{j=1}^m b_j e'_j, \end{aligned}$$

mida oligi tarvis tõestada. □

10.4 Lineaarkujutuste vektorruum

Lineaarkujutuste hulga saab loomulikult viisil muuta vektorruumiks.

Definitsioon 10.13 Olgu V_1 ja V_2 vektorruumid üle korpuse K, olgu $\varphi, \psi \in \mathrm{Hom}(V_1, V_2)$ ja $k \in K$. Defineerime kujutused $\varphi + \psi, k\varphi : V_1 \to V_2$ võrdustega

$$\begin{aligned}(\varphi + \psi)(a) &:= \varphi(a) + \psi(a),\\ (k\varphi)(a) &:= k\varphi(a),\end{aligned}$$

$a \in V_1$.

Selliste definitsioonide puhul öeldakse, et lineaarkujutuste liitmine ning lineaarkujutuse ja skalaari korrutis on defineeritud *punktiviisiliselt*. Selleks et leida $\varphi + \psi$ n.ö. punktis a, leiame φ ja ψ punktis a ning liidame tulemused. Analoogiliselt $k\varphi$ korral.

Lause 10.14 *Kui V_1 ja V_2 vektorruumid üle korpuse K, siis hulk* $\mathrm{Hom}(V_1, V_2)$ *on vektorruum eespool defineeritud liitmise ja skalaaridega korrutamise suhtes.*

Tõestus. Kontrollime kõigepealt, et $\varphi + \psi$ ja $k\varphi$ on lineaarkujutused. Tõepoolest,

$$\begin{aligned}(\varphi + \psi)(a + b) &= \varphi(a + b) + \psi(a + b) = \varphi(a) + \varphi(b) + \psi(a) + \psi(b)\\ &= \varphi(a) + \psi(a) + \varphi(b) + \psi(b) = (\varphi + \psi)(a) + (\varphi + \psi)(b),\\ (\varphi + \psi)(la) &= \varphi(la) + \psi(la) = l\varphi(a) + l\psi(a) = l(\varphi(a) + \psi(a)) = l((\varphi + \psi)(a))\\ (k\varphi)(a + b) &= k(\varphi(a + b)) = k(\varphi(a) + \varphi(b)) = k\varphi(a) + k\varphi(b) = (k\varphi)(a) + (k\varphi)(b),\\ (k\varphi)(la) &= k(\varphi(la)) = k(l\varphi(a)) = (kl)\varphi(a) = (lk)\varphi(a) = l(k\varphi(a)) = l((k\varphi)(a))\end{aligned}$$

iga $a, b \in V_1$ ja $l \in K$ korral. Seega on meil tegemist algebraliste tehetega hulgal $\mathrm{Hom}(V_1, V_2)$.

Veendume, et on täidetud vektorruumi definitsiooni tingimused. Kõigepealt märgime, et hulk $\mathrm{Hom}(V_1, V_2)$ ei ole tühi, sest ta sisaldab nullkujutust 0.

VR1. Olgu $\varphi, \psi, \chi \in \mathrm{Hom}(V_1, V_2)$. Siis iga $a \in V_1$ korral

$$\begin{aligned}((\varphi + \psi) + \chi)(a) &= (\varphi + \psi)(a) + \chi(a) = (\varphi(a) + \psi(a)) + \chi(a)\\ &= \varphi(a) + (\psi(a) + \chi(a)) = \varphi(a) + (\psi + \chi)(a) = (\varphi + (\psi + \chi))(a),\end{aligned}$$

mis tähendab, et $(\varphi + \psi) + \chi = \varphi + (\psi + \chi)$. Analoogiliselt saab näidata, et $\varphi + \psi = \psi + \varphi$, s.t. et kehtib VR4.

VR2. Olgu $\varphi \in \mathrm{Hom}(V_1, V_2)$. Siis iga $a \in V_1$ korral

$$(\varphi + 0)(a) = \varphi(a) + 0(a) = \varphi(a) + 0 = \varphi(a)$$

ehk $\varphi + 0 = \varphi$. See tähendab, et nullkujutus on nullelement lineaarkujutuste liitmise suhtes.

VR3. Olgu $\varphi \in \mathrm{Hom}(V_1, V_2)$. Defineerime kujutuse $-\varphi : V_1 \to V_2$ võrdusega

$$(-\varphi)(a) := -\varphi(a),$$

$a \in V_1$. Siis iga $a \in V_1$ korral

$$(\varphi + (-\varphi))(a) = \varphi(a) + (-\varphi)(a) = \varphi(a) + (-\varphi(a)) = 0,$$

mis tähendab, et $\varphi + (-\varphi) = 0$ ja seega $-\varphi$ on φ vastandelement liitmise suhtes.

VR5. Olgu $\varphi, \psi \in \mathrm{Hom}(V_1, V_2)$ ja $k \in K$. Siis iga $a \in V_1$ korral

$$\begin{aligned}(k(\varphi+\psi))(a) &= k((\varphi+\psi)(a)) = k(\varphi(a)+\psi(a)) = k\varphi(a)+k\psi(a)\\ &= (k\varphi)(a)+(k\psi)(a) = (k\varphi+k\psi)(a)\end{aligned}$$

ja seega $k(\varphi+\psi) = k\varphi + k\psi$.

Ülejäänud tingimuste kontroll on analoogiline. □

Nii saadud lineaarkujutuste vektorruumid ja maatriksite vektorruumid on omavahel väga tihedalt seotud.

Definitsioon 10.15 Olgu V_1 ja V_2 vektoruumid üle korpuse K. Neid vektorruume nimetatakse **isomorfseteks**, kui leidub bijektiivne lineaarkujutus $f : V_1 \to V_2$. Tähistatakse $V_1 \cong V_2$.

Teoreem 10.16 *Olgu V_1 n-mõõtmeline ja V_2 m-mõõtmeline vektorruum üle korpuse K. Siis vektorruumid* $\mathrm{Hom}(V_1, V_2)$ *ja* $\mathrm{Mat}_{m,n}(K)$ *on isomorfsed.*

Tõestus. Olgu $e = \{e_1, \ldots, e_n\}$ vektorruumi V_1 baas ja $e' = \{e'_1, \ldots, e'_m\}$ vektorruumi V_2 baas. Defineerime kujutuse

$$f : \mathrm{Hom}(V_1, V_2) \longrightarrow \mathrm{Mat}_{m,n}(K)$$

võrdusega

$$f(\varphi) := A_\varphi^{e,e'},$$

$\varphi \in \mathrm{Hom}(V_1, V_2)$.

Veendume, et f on lineaarkujutus.

LK1. Olgu $\varphi, \psi \in \mathrm{Hom}(V_1, V_2)$. Siis lause 6.47 põhjal

$$\overline{(\varphi+\psi)(e_i)}_{e'} = \overline{\varphi(e_i)+\psi(e_i)}_{e'} = \overline{\varphi(e_i)}_{e'} + \overline{\psi(e_i)}_{e'}$$

iga $i \in \{1, \ldots, n\}$ korral, s.t. maatriksi $A_{\varphi+\psi}^{e,e'}$ i-s veerg on maatriksite $A_\varphi^{e,e'}$ ja $A_\psi^{e,e'}$ i-ndate veergude summa. Järelikult $A_{\varphi+\psi}^{e,e'} = A_\varphi^{e,e'} + A_\psi^{e,e'}$ ja

$$f(\varphi+\psi) = A_{\varphi+\psi}^{e,e'} = A_\varphi^{e,e'} + A_\psi^{e,e'} = f(\varphi) + f(\psi).$$

LK2. Selle tingimuse kontroll on analoogiline.

Oletame nüüd, et $\varphi \in \mathrm{Ker}\, f$. Siis $f(\varphi) = A_\varphi^{e,e'}$ on nullmaatriks, mis tähendab, et $\varphi(e_i) = 0$ iga $i \in \{1, \ldots, n\}$ korral. Kui nüüd $a = a_1e_1 + \ldots + a_ne_n \in V_1$ on suvaline vektor, siis

$$\varphi(a) = a_1\varphi(e_1) + \ldots + a_n\varphi(e_n) = 0 + \ldots + 0 = 0.$$

See tähendab, et φ on nullteisendus ja me oleme näidanud, et $\mathrm{Ker}\, f = \{0\}$. Lause 10.8 põhjal on f üksühene.

Olgu lõpuks $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(K)$. Tänu lausele 10.5 leidub selline lineaarkujutus $\varphi : V_1 \to V_2$, mille korral

$$\varphi(e_j) = \sum_{i=1}^{m} a_{ij}e'_i,$$

kus $j = 1, \ldots, n$. Selle lineaarkujutuse korral $f(\varphi) = A$. Seega oleme näidanud, et f on pealekujutus ja kokkuvõttes on φ vektorruumide isomorfism. □

10.5 Lineaarteisenduste ring

Olgu V vektorruum üle korpuse K. Vektorruumi V lineaarteisenduste korrutamine defineeritakse järjestrakendamise abil:

$$(\psi\varphi)(a) := \psi(\varphi(a))$$

$\psi, \varphi \in \mathrm{End}(V)$, $a \in V$.

Lause 10.17 *Hulk* $\mathrm{End}(V)$ *on ring lineaarteisenduste liitmise ja korrutamise suhtes.*

TÕESTUS. Veendume, et lineaarteisenduste korrutis on ka lineaarteisendus. Kui V on vektorruum üle korpuse K, $\varphi, \psi \in \mathrm{End}(V)$, $a, b \in V$ ja $k \in K$, siis

$$\begin{aligned}(\psi\varphi)(a+b) &= \psi(\varphi(a+b)) = \psi(\varphi(a)+\varphi(b)) = \psi(\varphi(a)) + \psi(\varphi(b)) = (\psi\varphi)(a) + (\psi\varphi)(b),\\ (\psi\varphi)(ka) &= \psi(\varphi(ka)) = \psi(k\varphi(a)) = k\psi(\varphi(a)) = (\psi\varphi)(a),\end{aligned}$$

mis tähendab, et $\psi\varphi \in \mathrm{End}(V)$.

Lause 10.14 tõestuses nägime, et $(\mathrm{End}(V), +)$ on Abeli rühm. Samuti teame, et hulga teisenduste korrutamine on assotsiatiivne ja samasusteisendus on selle korrutamise suhtes ühikelement. Seega jääb veel kontrollida, et kehtivad distributiivsuse seadused.

Olgugi $\varphi, \psi, \chi \in \mathrm{End}(V)$. Siis iga $a \in V$ korral

$$\begin{aligned}(\varphi(\psi+\chi))(a) &= \varphi((\psi+\chi)(a)) = \varphi(\psi(a)+\chi(a)) = \varphi(\psi(a)) + \varphi(\chi(a))\\ &= (\varphi\psi)(a) + (\varphi\chi)(a) = (\varphi\psi + \varphi\chi)(a),\\ ((\psi+\chi)\varphi)(a) &= (\psi+\chi)(\varphi(a)) = \psi(\varphi(a)) + \chi(\varphi(a)) = (\psi\varphi)(a) + (\chi\varphi)(a)\\ &= (\psi\varphi + \chi\varphi)(a).\end{aligned}$$

Järelikult $\varphi(\psi+\chi) = \varphi\psi + \varphi\chi$ ja $(\psi+\chi)\varphi = \psi\varphi + \chi\varphi$. □

Lineaarteisenduste ringid on seotud ruutmaatriksite ringidega.

Teoreem 10.18 *Olgu* V *n-mõõtmeline vektorruum üle korpuse* K. *Siis ringid* $\mathrm{End}(V)$ *ja* $\mathrm{Mat}_n(K)$ *on isomorfsed.*

TÕESTUS. Olgu $e = \{e_1, \ldots, e_n\}$ vektorruumi V baas. Defineerime kujutuse

$$f : \mathrm{End}(V) \longrightarrow \mathrm{Mat}_n(K)$$

võrdusega

$$f(\varphi) := A^e_\varphi,$$

$\varphi \in \mathrm{End}(V)$. Teoreemi 10.16 tõestuses nägime, et selline kujutus on bijektiivne ja säilitab liitmise. On selge, et $f(1_V) = E$, kus ühikmaatriks E on ringi $\mathrm{Mat}_n(K)$ ühikelement.

Jääb veel näidata, et mistahes $\varphi, \psi \in \mathrm{End}(V)$ korral $f(\psi\varphi) = f(\psi)f(\varphi)$ ehk $A^e_\psi A^e_\varphi = A^e_{\psi\varphi}$. Maatriksi $A^e_{\psi\varphi}$ i-s veerg on definitsiooni järgi $\overline{(\psi\varphi)(e_i)}_e$. Lause 10.12 põhjal

$$\overline{(\psi\varphi)(e_i)}_e = \overline{\psi(\varphi(e_i))}_e = A^e_\psi \overline{\varphi(e_i)}_e = A^e_\psi(A^e_\varphi \overline{e_i}_e) = (A^e_\psi A^e_\varphi)\overline{e_i}_e.$$

Kuna $e_i = 0 \cdot e_1 + \ldots + 0 \cdot e_{i-1} + 1 \cdot e_i + 0 \cdot e_{i+1} + \ldots + 0 \cdot e_n$, siis maatriks $\overline{e_i}_e$ on veerg, mille i-ndal kohal on 1 ja kõik ülejäänud komponendid on nullid. Korrutades maatriksi $A^e_\psi A^e_\varphi$

paremalt sellise veeruga saame maatriksi $A^e_\psi A^e_\varphi$ i-nda veeru. Seega maatriksite $A^e_{\psi\varphi}$ ja $A^e_\psi A^e_\varphi$ vastavad veerud on võrdsed, mis tähendab, et ka need maatriksid on võrdsed. □

Võtame lõpuks veelkord lühidalt kokku tähtsamad seosed lineaarkujutuste ja maatriksite vahel. Niisiis

$$\boxed{A^{e,e'}_{\varphi+\psi} = A^{e,e'}_\varphi + A^{e,e'}_\psi,}$$

$$\boxed{A^{e,e'}_{k\varphi} = kA^{e,e'}_\varphi,}$$

$$\boxed{A^e_{\psi\varphi} = A^e_\psi A^e_\varphi.}$$

10.6 Sarnased maatriksid

Definitsioon 10.19 Maatrikseid $A, B \in \mathrm{Mat}_n(K)$ nimetatakse **sarnasteks** (ja kirjutatakse $A \sim B$), kui leidub selline regulaarne maatriks $T \in \mathrm{Mat}_n(K)$, et $B = T^{-1}AT$.

Lemma 10.20 *Maatriksite sarnasuse seos on ekvivalentsiseos.*

Tõestus. Iga maatriksi $A \in \mathrm{Mat}_n(K)$ korral $A = E^{-1}AE$, kusjuures ühikmaatriks E on regulaarne. Seega $A \sim A$ ja seos $\sim$ on refleksiivne.

Olgu $A \sim B$. Siis $B = T^{-1}AT$, kus $T \in \mathrm{Mat}_n(K)$ on regulaarne maatriks. Järelikult $A = TBT^{-1} = (T^{-1})^{-1}BT^{-1}$, kus ka T^{-1} on regulaarne. Seega $B \sim A$ ja seos $\sim$ on sümmeetriline.

Kui $A \sim B$ ja $B \sim C$, siis leiduvad sellised regulaarsed maatriksid $T, U \in \mathrm{Mat}_n(K)$, et $B = T^{-1}AT$ ja $C = U^{-1}BU$. Järelikult

$$C = U^{-1}BU = U^{-1}T^{-1}ATU = (TU)^{-1}A(TU),$$

kus ka maatriks TU on regulaarne. See tähendab, et $A \sim C$ ja seos $\sim$ on transitiivne. □

Definitsioon 10.21 Olgu V n-mõõtmeline vektorruum üle korpuse K ja olgu $e = \{e_1, \ldots, e_n\}$, $e' = \{e'_1, \ldots, e'_n\}$ vektorruumi V kaks baasi. **Üleminekumaatriksiks** baasilt e baasile e' nimetatakse maatriksit, mille i-ndas veerus ($i \in \{1, \ldots, n\}$) on vektori e'_i koordinaadid baasi e suhtes. Seda maatriksit tähistatakse $T^{e,e'}$.

Seega kui $T^{e,e'} = (t_{ij}) \in \mathrm{Mat}_n(K)$, siis kehtivad seosed

$$e'_i = t_{1i}e_1 + \ldots + t_{ni}e_n = \sum_{j=1}^{n} t_{ji}e_j, \tag{50}$$

$i \in \{1, \ldots, n\}$.

Lemma 10.22 *Üleminekumaatriks ühelt baasilt teisele on regulaarne.*

Tõestus. Vaatleme üleminekumaatriksit $T^{e,e'}$. Tänu lause 7.13 analoogile veergude jaoks võime öelda, et maatriks $T^{e,e'}$ on regulaarne, kui tema veeruvektorite süsteem on lineaarselt sõltumatu. Viimane kehtib parajasti siis, kui ükski veeruvektor ei avaldu eelmiste lineaarkombinatsioonina. Kui oletaksime, et i-s veeruvektor avaldub eelmiste lineaarkombinatsioonina, siis ka vektor e'_i avalduks vektorite $e'_1, \ldots, e'_{i-1}$ lineaarkombinatsioonina. Seda aga ei saa olla, sest baasivektorid on lineaarselt sõltumatud. □

Tõestame nüüd tulemuse, mis näitab, kuidas on omavahel seotud lineaarteisenduse φ maatriksid erinevate baaside e ja e' suhtes.

Teoreem 10.23 *Olgu V n-mõõtmeline vektorrrum üle korpuse K, olgu e, e' selle vektorruumi baasid ja olgu φ selle vektorruumi lineaarteisendus. Siis*

$$\boxed{A_\varphi^{e'} = T^{-1} A_\varphi^e T,}$$

kus $T = T^{e,e'}$.

Tõestus. Vastavalt teoreemile 10.18 on kujutus

$$f : \mathrm{End}(V) \to \mathrm{Mat}_n(K), \quad \varphi \mapsto A_\varphi^e$$

ringide isomorfism. Lemma 10.22 põhjal on maatriks T regulaarne ja seega leidub tal pöördmaatriks T^{-1}. Kuna f on pealekujutus, siis leiduvad sellised $\psi, \chi \in \mathrm{End}(V)$, et

$$T = f(\psi) = A_\psi^e, \quad T^{-1} = f(\chi) = A_\chi^e.$$

Siis

$$f(1_V) = E = TT^{-1} = f(\psi)f(\chi) = f(\psi\chi)$$

ja analoogiliselt $f(1_V) = f(\chi\psi)$. Kuna f on üksühene, siis $\psi\chi = 1_V = \chi\psi$ ehk teiste sõnadega $\chi = \psi^{-1}$. Niisiis $f(\psi^{-1}) = T^{-1}$.

Paneme tähele, et

$$T^{-1} A_\varphi^e T = f(\psi^{-1})f(\varphi)f(\psi) = f(\psi^{-1}\varphi\psi) = A_{\psi^{-1}\varphi\psi}^e.$$

Uurime nüüd maatriksit $A_{\psi^{-1}\varphi\psi}^e$. Olgu $A_\varphi^{e'} = (b_{ij})$, s.t. $\varphi(e_i') = \sum_{j=1}^n b_{ji} e_j'$ iga $i \in \{1, \ldots, n\}$ korral. Kuna $A_\psi^e = T$, siis võrreldes nende maatriksite i-ndaid veerge ja kasutades võrdust (50) saame, et

$$\psi(e_i) = t_{1i}e_1 + \ldots + t_{ni}e_n = e_i' \tag{51}$$

iga $i \in \{1, \ldots, n\}$ korral ning järelikult $\psi^{-1}(e_i') = e_i$ iga $i \in \{1, \ldots, n\}$ korral. Seda arvestades võime kirjutada

$$\begin{aligned}(\psi^{-1}\varphi\psi)(e_i) &= \psi^{-1}(\varphi(\psi(e_i))) = \psi^{-1}(\varphi(e_i')) = \psi^{-1}\left(\sum_{j=1}^n b_{ji} e_j'\right) \\ &= \sum_{j=1}^n b_{ji}\psi^{-1}\left(e_j'\right) = \sum_{j=1}^n b_{ji} e_j.\end{aligned}$$

See näitab, et $A_{\psi^{-1}\varphi\psi}^e = (b_{ij})$ ehk $T^{-1}A_\varphi^e T = A_\varphi^{e'}$. □

Järeldus 10.24 *Maatriksid $A, B \in \mathrm{Mat}_n(K)$ on sarnased parajasti siis, kui nad on mingi vektorruumi V (üle K) mingi lineaarteisenduse maatriksid mingite baaside suhtes.*

Tõestus. Piisavus. See on tõestatud teoreemis 10.23.
Tarvilikkus. Olgu maatriksid $A, B \in \mathrm{Mat}_n(K)$ sarnased, s.t. $B = T^{-1}AT$, kus $T = (t_{ij}) \in \mathrm{Mat}_n(K)$ on regulaarne maatriks. Vaatleme vektorruumi K^n ja selle baasi e, mis koosneb vektoritest

$$\begin{aligned}e_1 &= (1, 0, 0, \ldots, 0), \\ e_2 &= (0, 1, 0, \ldots, 0), \\ &\ldots \\ e_n &= (0, 0, 0, \ldots, 1).\end{aligned}$$

Siis teoreemi 10.18 põhjal leidub lineaarteisendus $\varphi \in \mathrm{End}(K^n)$ nii, et $A = A^e_\varphi$. Iga $i \in \{1, \ldots, n\}$ korral olgu

$$e'_i := t_{1i}e_1 + \ldots + t_{ni}e_n = (t_{1i}, \ldots, t_{ni}),$$

s.t. $e'_i \in K^n$ on maatriksi T i-s veeruvektor. Kuna T on regulaarne, siis on tema veeruvektorid $e'_1, \ldots, e'_n$ lineaarselt sõltumatud ning järelikult on $e' = \{e'_1, \ldots, e'_n\}$ vektorruumi K^n baas. Üleminekumaatriksi definitsiooni põhjal $T = T^{e,e'}$. Seega

$$B = T^{-1}AT = T^{-1}A^e_\varphi T = A^{e'}_\varphi$$

ning A ja B on lineaarteisenduse φ maatriksid baaside e ja e' suhtes. □

10.7 Karakteristlik polünoom

Seome nüüd iga maatriksiga teatud polünoomi.

Definitsioon 10.25 Maatriksi $A \in \mathrm{Mat}_n(K)$ **karakteristlikuks polünoomiks** nimetatakse polünoomi $|A - \lambda E| \in K[\lambda]$.

Näeme, et A karakteristliku polünoomi kordajateks on K elemendid ja tundmatuks on λ.

Näide 10.26 Maatriksi $A = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R})$ karakteristlik polünoom on

$$\begin{aligned} |A - \lambda E| &= \left| \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right| = \left| \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right| = \begin{vmatrix} 2-\lambda & 1 \\ -1 & -\lambda \end{vmatrix} \\ &= \lambda^2 - 2\lambda + 1. \end{aligned}$$

Üldjuhul, kui $A = (a_{ij}) \in \mathrm{Mat}_n(K)$, siis

$$|A - \lambda E| = \begin{vmatrix} a_{11} - \lambda & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - \lambda & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \lambda \end{vmatrix}.$$

Determinandi definitsioonist järeldub kergesti, et maatriksi $A \in \mathrm{Mat}_n(K)$ karakteristliku polünoomi aste on n ja pealiige on $(-1)^n\lambda^n$.

Lause 10.27 *Sarnaste maatriksite karakteristlikud polünoomid on võrdsed.*

Tõestus. Olgu maatriksid $A, B \in \mathrm{Mat}_n(K)$ sarnased. Siis $B = T^{-1}AT$, kus T on mingi regulaarne maatriks. Kasutades maatriksite ja determinantide omadusi saame, et

$$\begin{aligned} |B - \lambda E| &= |T^{-1}AT - T^{-1}(\lambda E)T| = |T^{-1}(AT - (\lambda E)T)| = |T^{-1}(A - \lambda E)T| \\ &= |T^{-1}||A - \lambda E||T| = |T^{-1}||T||A - \lambda E| = |T^{-1}T||A - \lambda E| = |E||A - \lambda E| \\ &= |A - \lambda E|. \end{aligned}$$

□

Definitsioon 10.28 Maatriksi $A \in \mathrm{Mat}_n(K)$ **omaväärtusteks** nimetatakse selle maatriksi karakteristliku polünoomi juuri.

Näide 10.29 Näites 10.26 vaadeldud maatriksi omaväärtusteks on polünoomi $\lambda^2 - 2\lambda + 1 = (\lambda - 1)^2$ juured. Seega on sellel maatriksil omaväärtus 1, mille kordsus on kaks.

10.8 Lineaarteisenduse omaväärtused ja omavektorid

Definitsioon 10.30 Olgu V vektorruum üle korpuse K ja olgu φ vektorruumi V lineaarteisendus. Vektorit $0 \neq a \in V$ nimetatakse lineaarteisenduse φ **omavektoriks**, kui leidub selline $\lambda \in K$, et

$$\varphi(a) = \lambda a.$$

Elementi λ nimetatakse sel juhul omavektorile a vastavaks **omaväärtuseks**.

Näide 10.31 Näites 10.3(4) vaadeldud peegeldamisteisenduse omaväärtusteks on 1 ja -1. Omaväärtusele 1 vastavad omavektorid on need nullist erinevad vektorid, mis on paralleelsed y-teljega. Omaväärtusele -1 vastavad omavektorid on need nullist erinevad vektorid, mis on paralleelsed x-teljega.

Vektorruumi samasusteisenduse ja nullteisenduse jaoks on kõik nullist erinevad vektorid omavektorid.

Definitsioon 10.32 Lineaarteisenduse **karakteristlikuks polünoomiks** nimetatakse selle lineaarteisenduse maatriksi karakteristlikku polünoomi.

Paneme tähele, et lause 10.27 põhjal ei sõltu lineaarteisenduse karakteristlik polünoom sellest, millise baasi suhtes me tema maatriksit vaatleme.

Teoreem 10.33 *Lineaarteisenduse omaväärtusteks on selle teisenduse karakteristliku polünoomi juured.*

Tõestus. Olgu V n-mõõtmeline vektorruum üle korpuse K baasiga e ja olgu φ vektorruumi V lineaarteisendus. Olgu $A = A^e_\varphi = (a_{ij}) \in \mathrm{Mat}_n(K)$. Siis lause 10.12 põhjal kehtib iga vektori $x \in V$ korral võrdus

$$\overline{\varphi(x)}_e = A^e_\varphi \overline{x}_e.$$

Tänu lausele 6.47 on iga $\lambda_0 \in K$ korral $\overline{\lambda_0 x}_e = \lambda_0 \overline{x}_e = (\lambda_0 E)\overline{x}_e$. Seega vektor $x \in V \setminus \{0\}$ on lineaarteisenduse φ omavektor parajasti siis, kui

$$A^e_\varphi \overline{x}_e = (\lambda_0 E)\overline{x}_e$$

ehk

$$(A^e_\varphi - \lambda_0 E)\overline{x}_e = \overline{0}_e$$

mingi $\lambda_0 \in K$ korral. Kui

$$\overline{x}_e = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix},$$

siis omavektorite x leidmine on samaväärne homogeense lineaarvõrrandisüsteemi

$$\begin{cases} (a_{11} - \lambda_0)x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + (a_{22} - \lambda_0)x_2 + \ldots + a_{2n}x_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + (a_{nn} - \lambda_0)x_n = 0 \end{cases} \tag{52}$$

nullist erinevate lahendite leidmisega. Element $\lambda_0 \in K$ on omaväärtus parajasti siis, kui sellel süsteemil leidub nullist erinev lahend.

Veendume, et süsteemil (52) leidub nullist erinev lahend parajasti siis, kui λ_0 on karakteristliku polünoomi juur. Kui selle süsteemi maatriksi determinant $|A - \lambda_0 E|$ on nullist erinev, siis on tegemist Crameri peajuhuga ja ainsaks lahendiks on nullvektor, mis ei saa olla omavektor. Seega, kui leidub nullist erinev lahend, siis $|A - \lambda_0 E| = 0$ ja λ_0 on karakteristliku polünoomi juur. Vastupidi, kui $|A - \lambda_0 E| = 0$, siis süsteemi maatriksi astak (s.t. nullist erinevate miinorite kõrgeim järk) $r < n$ ja lahendite fundamentaalsüsteemis leidub $n - r > 1$ lineaarselt sõltumatut vektorit, mis peavad olema nullist erinevad. Kõik need vektorid on omavektorid. □

Teoreemi 10.33 tõestuse põhjal saame järgmise eeskirja omavektorite leidmiseks.

1. Leiame lineaarteisenduse φ maatriksi A mingi baasi e suhtes.
2. Leiame polünoomi $|A - \lambda E|$ juured $\lambda_1, \ldots, \lambda_m$.
3. Iga λ_i ($i \in \{1, \ldots, m\}$) jaoks lahendame homogeense lineaarvõrrandisüsteemi maatriksiga $A - \lambda_i E$. Selle süsteemi nullist erinevad lahendivektorid on parajasti lineaarteisenduse φ omavektorite koordinaatide vektorid baasi e suhtes.

Võib küsida, et milliste baaside suhtes on lineaarteisenduse maatriks võimalikult lihtne. Ühtedeks lihtsamateks maatriksiteks on diagonaalmaatriksid. Osutub, et kehtib järgmine lause.

Lause 10.34 *Lineaarteisenduse φ maatriks baasi $\{e_1, \ldots, e_n\}$ suhtes on diagonaalmaatriks parajasti siis, kui see baas koosneb teisenduse φ omavektoritest.*

Tõestus. Olgu φ vektorruumi V (üle korpuse K) lineaarteisendus ja olgu $e = \{e_1, \ldots, e_n\}$ vektorruumi V baas.
Tarvilikkus. Kui

$$A_\varphi^e = \begin{pmatrix} k_1 & 0 & \ldots & 0 \\ 0 & k_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & k_n \end{pmatrix},$$

siis lineaarteisenduse maatriksi definitsiooni tõttu iga $i \in \{1, \ldots, n\}$ korral $\varphi(e_i) = k_i e_i$, mis tähendab, et $e_1, \ldots, e_n$ on φ omavektorid.
Piisavus. Olgu $e_1, \ldots, e_n$ teisenduse φ omavektorid. Siis leiduvad $k_1, \ldots, k_n \in K$ nii, et $\varphi(e_i) = k_i e_i$ iga $i \in \{1, \ldots, n\}$ korral. Seega A_φ^e on diagonaalmaatriks, mille peadiagonaalil on elemendid $k_1, \ldots, k_n$. □

Indeks

Kasutatud kirjandus

1. M. Kilp, Algebra I, Eesti Matemaatika Selts, Tartu, 2005.
2. K. Kaarli, Algebra I loengute slaidid,
http://math.ut.ee/pmi/kursused/algebraI/algebra1_ slides.pdf .
3. A. Parring, Algebra ja Geomeetria loengukonspekt,
http://math.ut.ee/pmi/kursused/ag/parring/.
4. G. Kangro, Kõrgem algebra I, RK "Teaduslik kirjandus", Tartu, 1948.
5. A. I. Kostrikin, Vvedenie v algebru, Nauka, Moskva, 1977 (vene keeles).